Firepower Threat Defense (FMC 管理) Version 6.4 初期セットアップガイド

Rev 1.0

2020/04

シスコシステムズ合同会社

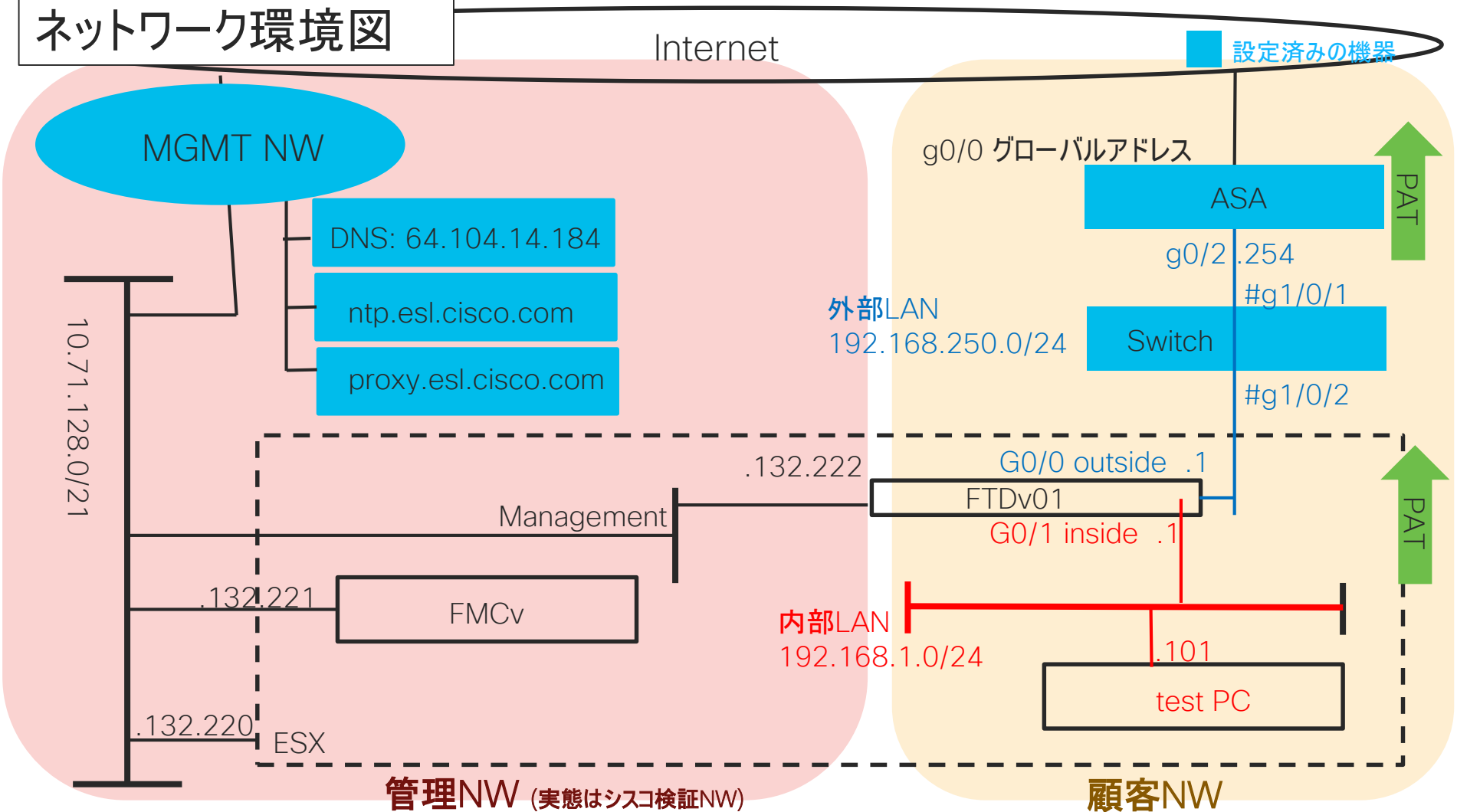
はじめに

- 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、2020年4月現在の情報に基づいており、FTD & FMCのソフトウェアは 6.4.0.xを、ハイパーバイザはVMware ESXi 6.5を利用しております。
- 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
DNS: 64.104.14.184
ntp.esl.cisco.com
proxy.esl.cisco.com
10.71.128.0/21
g0/0 グローバルアドレス
ASA
PAT
g0/2 .254
#g1/0/1
外部LAN
192.168.250.0/24
Switch
#g1/0/2
.132.222
G0/0 outside .1
FTDv01
Management
G0/1 inside .1
PAT
.132.221
FMCv
内部LAN
192.168.1.0/24
.101
test PC
.132.220
ESX
管理NW (実態はシスコ検証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。
- Prefilter Policyにて192.168.1.0/24が送信元 or 宛先の通信は以降のセキュリティ検査をバイパスするようにする。
- 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、File PolicyにてMalwareをブロックするようにする。
- 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。

当ガイドのシナリオ(続き)

- SSL Policyにて内部から外部への通信を復号し、セキュリティ検査を適用する。
- FTDvのバックアップを取得し、有事の際のリストアを検証する。
- Syslog, アラート, レポーティングの設定を行う。
- FTDvを冗長構成にする。
- <<Appendix>> にはこのシナリオには含まれないTIPSを記載

目次

1. FMCvとFTDvのインストール
2. FMCとFTDその他初期設定
3. シグネチャ及び各種DBの更新
4. スマートライセンスの適用
5. Routed FirewallとNetwork Discoveryの設定
6. Prefilterの設定
7. Intrusion Policyの設定
8. Malware & File Policyの設定
9. Access Control Policyの設定
10. TLS Decryptionの設定
11. バックアップの設定とリストアの方法
12. Syslog・レポート・アラートの設定
13. FTD High Availabilityの設定

<< Appendix >>

1. マルチインスタンスの作成
2. FMCアプライアンスHA構成のアップグレード方法

その他追加予定有り

1. FTDvとFMCv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

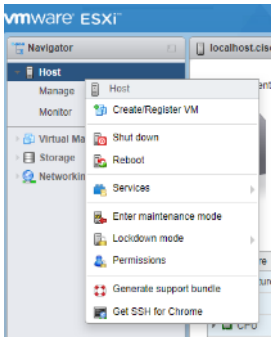
① FTDの登録

ステップ 1-1: OVFのデプロイと Web GUIアクセス

1. https://software.cisco.com/ から”Software Download”に進む。
2. Select a Productのテキストフィールドで Firepower Management Center 入力する。結果表示される選択肢の中からここでは Firepower Management Center Virtual Appliance を選択。Firepower Management Center Software を選択しFMCのtarファイルを取得し展開する。
   - ソフトウェアはその時適切なものを選択すること。

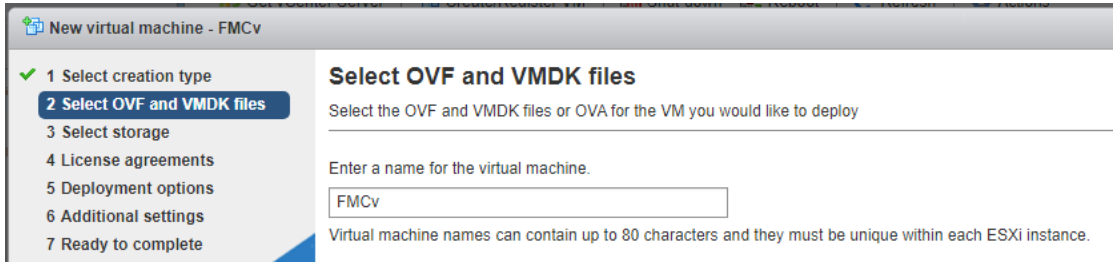
FMCv: VMware install package for ESXi 6.0 and 6.5 24-Apr-2019 2210.28 MB
Cisco_Firepower_Mgmt_Center_Virtual_VMware-6.4.0-102.tar.gz

3. vSphere Clientで展開したOVFをデプロイしていく



ステップ 1-2: OVFのデプロイと Web GUIアクセス

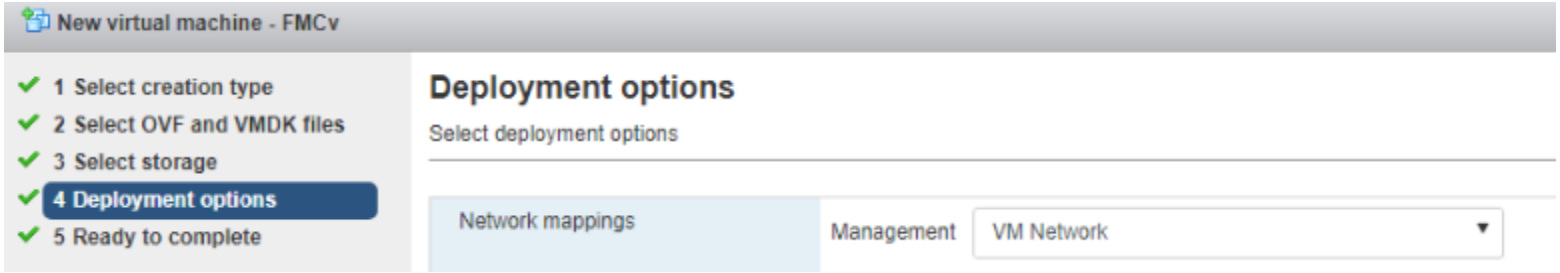
1. 仮想FMCに名前をつける



2. 同じ画面で以下をクリックし先ほど展開したOVFとVMDKを選択しNextをクリック

ステップ 1-3: OVFのデプロイと Web GUIアクセス

1. 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

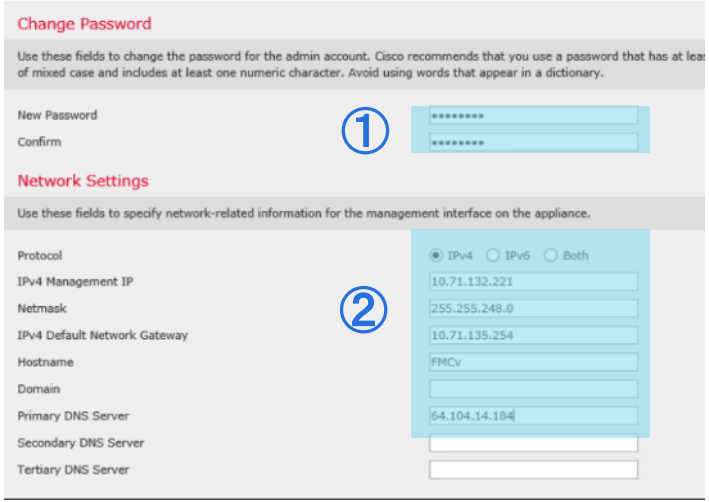


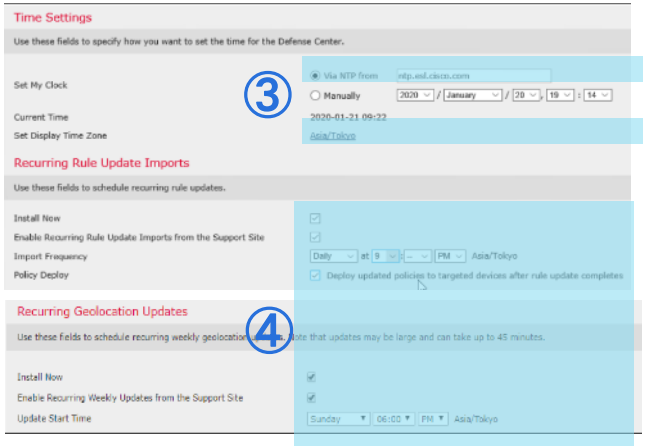
2. その他デフォルトの設定値でデプロイ
3. ブラウザで FMCのデフォルトのIPアドレスにHTTPSアクセス
   https://192.168.45.45/
   ユーザ名： admin
   パスワード： Admin123

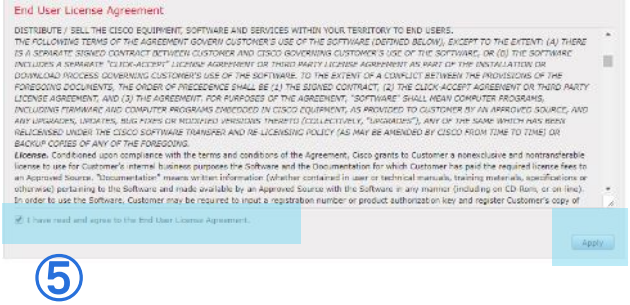
CLIでFMCのIPアドレスを変更する方法もあるがここでは割愛

ステップ 2-1:初期設定

Firepower Management Center







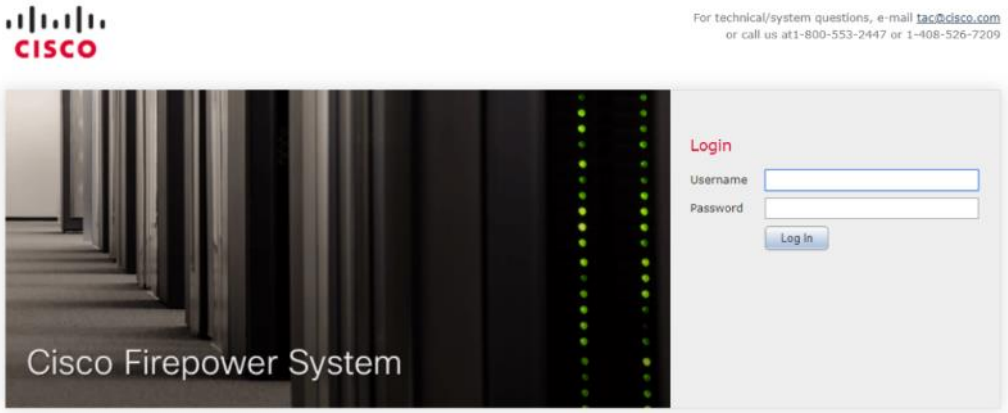
① adminパスワードの変更
② FMCのIPアドレス、デフォルトゲートウェイ、ホスト名、DNSサーバを入力
③ NTPサーバのIPアドレスまたはFQDNを入力、Time Zoneの変更
④ 更新内容の設定を画面のように入力
⑤ 最後にライセンス契約(EULA)にチェックを入れ “Apply”を選択

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

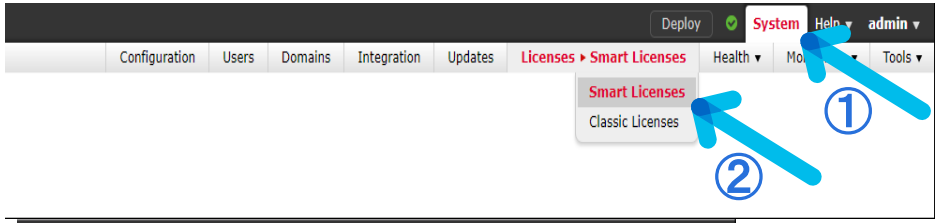
ステップ 2-2: 設定したIPアドレスにアクセス

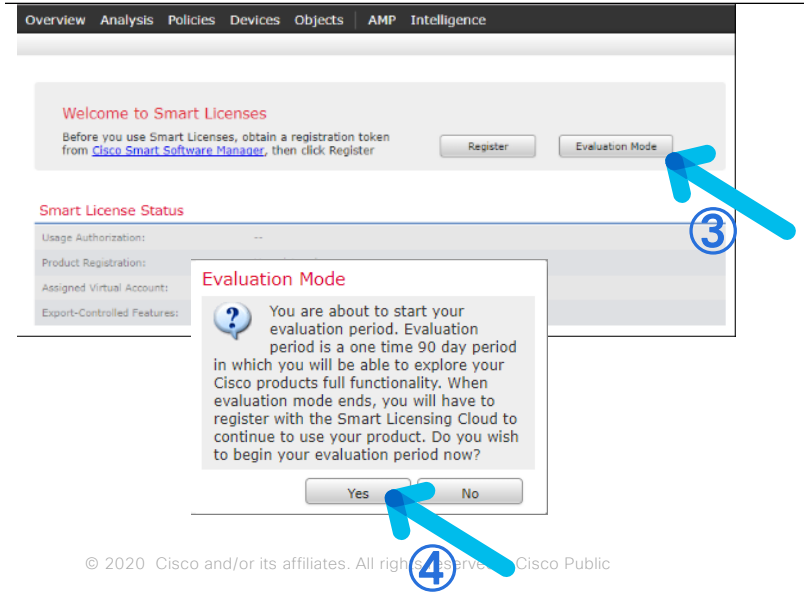
- **初期設定で入力した IP アドレスと adminパスワードを使い FMCの Web GUI へブラウザでHTTPSアクセスしログイン**

  ※ 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2-1で 10.71.132.221に変更いただいているため、ここでは注意)

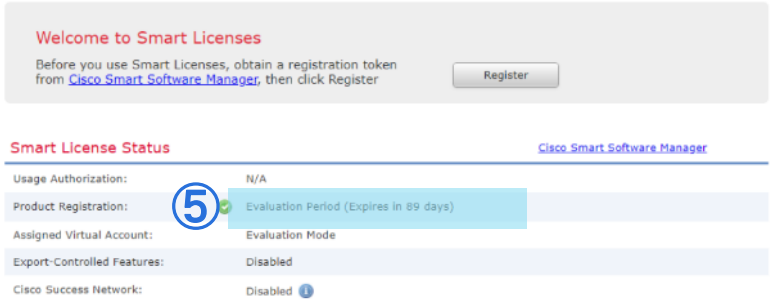


ステップ 3: ライセンスの追加





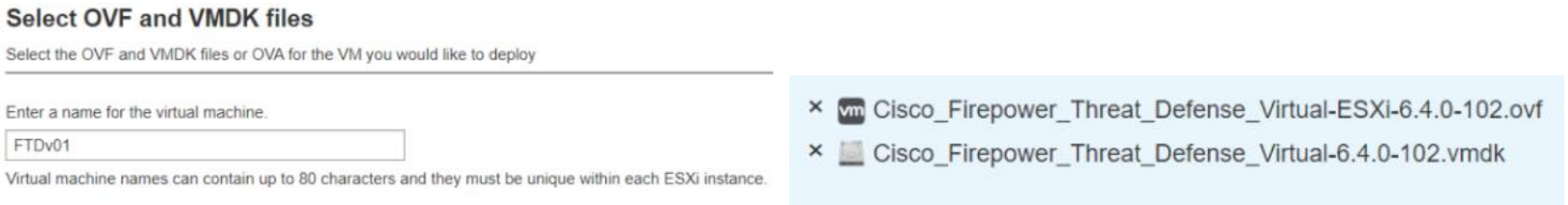
ここではEvaluation Modeを利用する。(Smart Licenseについては後述)
Evaluation Modeでは、90日間AnyConnect以外の全機能が利用可能。



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

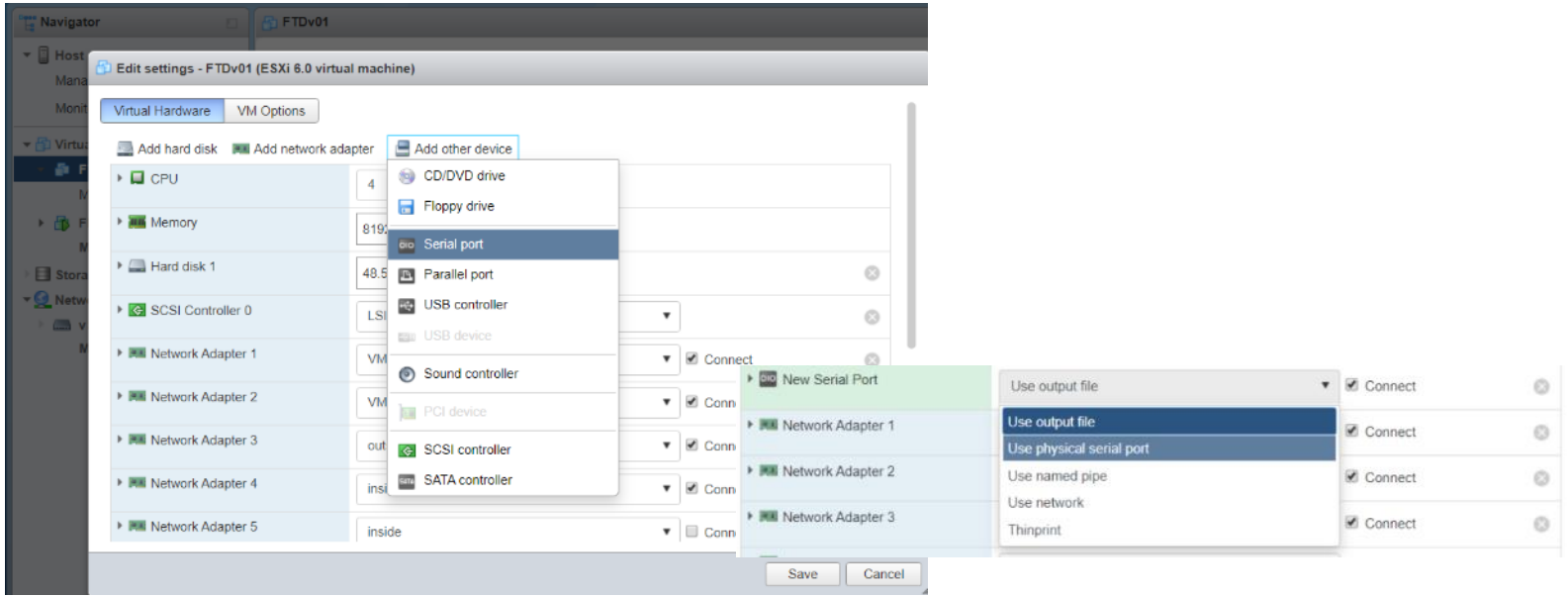
ステップ 1-1: OVFのデプロイ

1. https://software.cisco.com/ から”Software Download”に進む。
2. Select a ProductのテキストフィールドでFirepower Threat DefenseやNGFWと入力する。結果表示される選択肢の中からここではFirepower NGFW Virtualを選択。Firepower Threat Defense (FTD) Softwareを選択しFTDのtarファイルを取得し展開する。
   - ソフトウェアバージョンはその時適切なものを選択すること。
3. FMCと同じ要領でOVFとVMDKファイルを選んでデプロイを進める



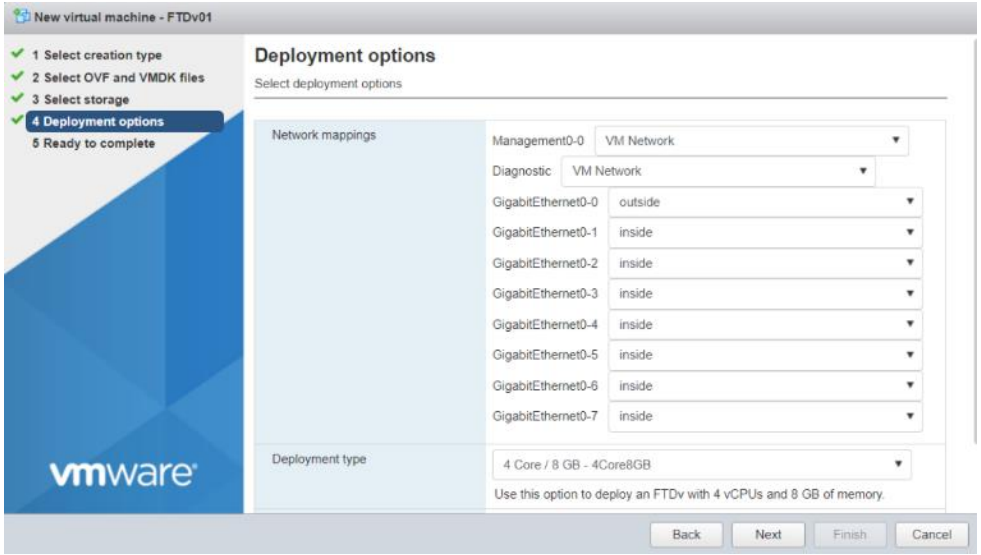
ステップ 1-3: OVFのデプロイ

1. FTDvの電源を落とした状態で右クリックし設定を編集にすすみ、シリアルポートを追加する



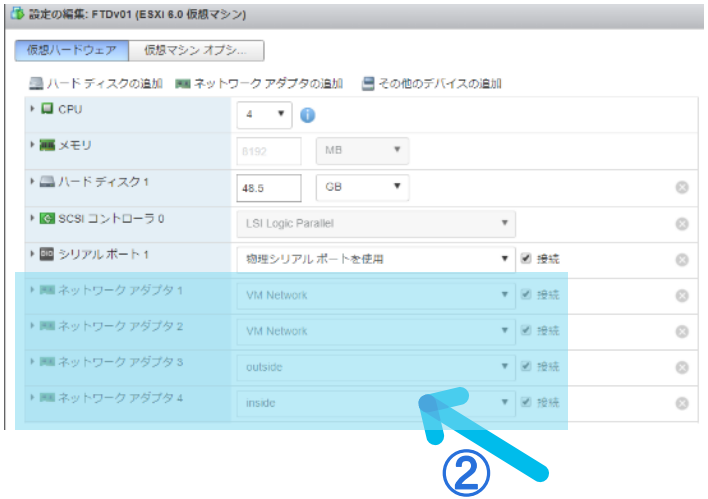
ステップ 1-2: OVFのデプロイ

1. FTDは管理用、Diagnosticインタフェースを管理ネットワークに所属させる (ESXi上のネットワークは作成済とする)



2. その他vSphere Client上での設定はデフォルトを使用し、電源を切った状態でデプロイ

ステップ 2-1: アダプタタイプの変更



① 作成したFTDを右クリックして編集
② FTDの仮想マシンのインタフェースをここではoutside, insideを割り当てて”接続にチェック”

ステップ 3-1: 初期設定

- vSphere Client上で デプロイした FTD の VMコンソールを開き、Login プロンプトが表示されたら以下のユーザーでログイン
  Username: admin
  Password: Admin123
  ※ユーザー名の入力の前に、Passwordを最初に求められた場合、Enter を一度入力すると以下のようにFirepower login : を表示される。username として admin と入力し、続けてPasswordを入力

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

- ライセンス契約(EULA)を [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

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

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

- Adminユーザ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]: 10.71.132.22
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 [192.168.45.1]: 10.7
1.135.254
Enter a fully qualified hostname for this system [firepower]: FTDv01
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220
.220]: 64.104.14.184
```

- **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

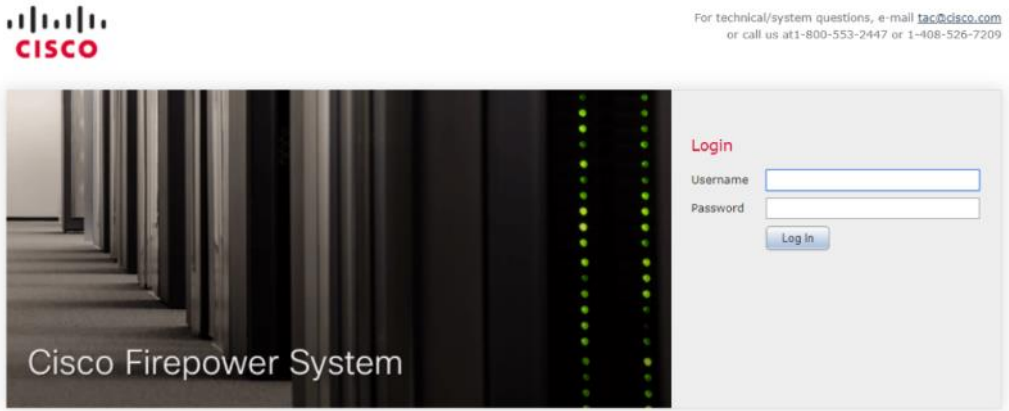
- **FMCのアドレスと登録キーを設定**
  以下のコマンドを使い、FMCへのデバイス登録の設定を行う
  後述のFMCからFTDをデバイス登録する際に、この登録キー(この例では “cisco”)が一致している必要あり

  configure manager add <ip address> <key>

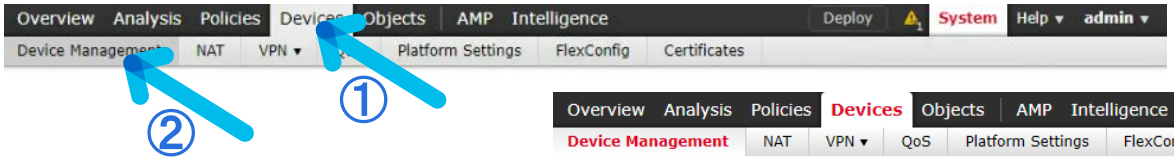
```
> configure manager add 10.71.132.221 cisco
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
```

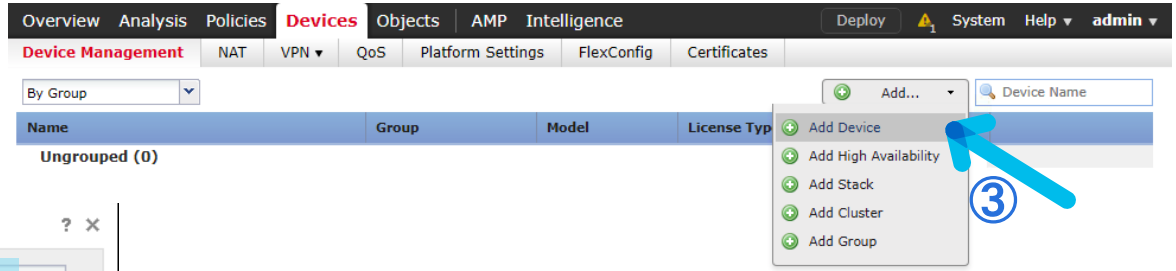
ステップ 1-1: FTDデバイスの登録

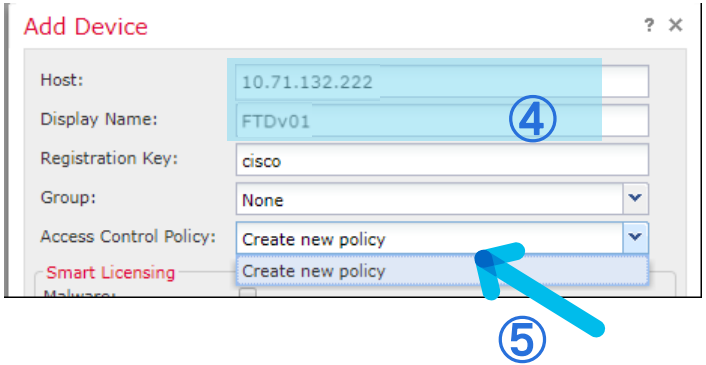
- **初期設定で入力した** IP **アドレス** (10.71.132.221) **と** admin**パスワードを使い** FMC**の** Web GUI **へブラウザで**HTTPS**アクセスしログイン**



ステップ 1-2: FTDデバイスの登録

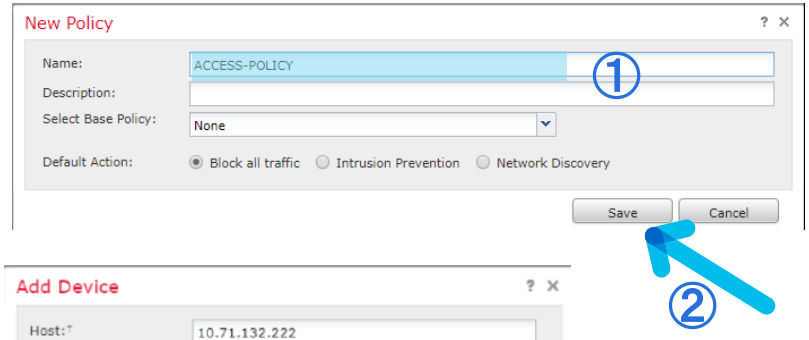


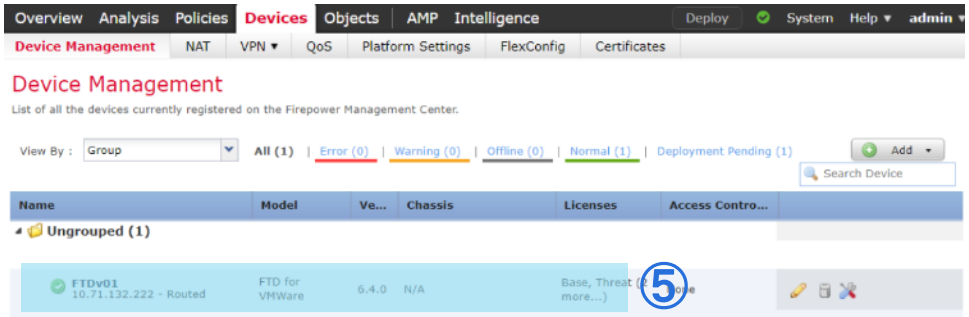




① GUI の上部にある Devices を選択
② Device Management を選択
③ Add Device を選択
④ FTD の IPアドレスと、登録キーを入力
⑤ “Create new Policy” を選択
引き続き、次のスライドを参照

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

2. FTDとFMCその他初期設定

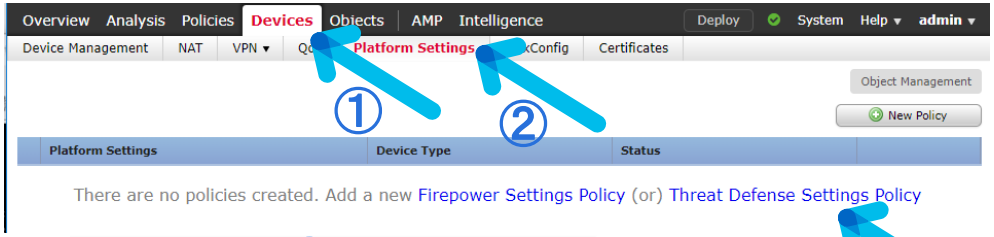
FTDとFMCその他初期設定に関して

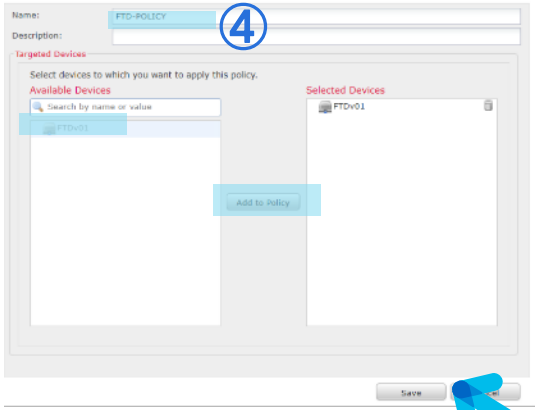
- FTDのネットワーク周りで行うべき最低限の設定を行う
  - Time Synchronization
  - Interface
  - *Routing*
  - *NAT*
  - *Access Control Policy*
  - *Network Discovery Policy*
  - *Pre-filter*

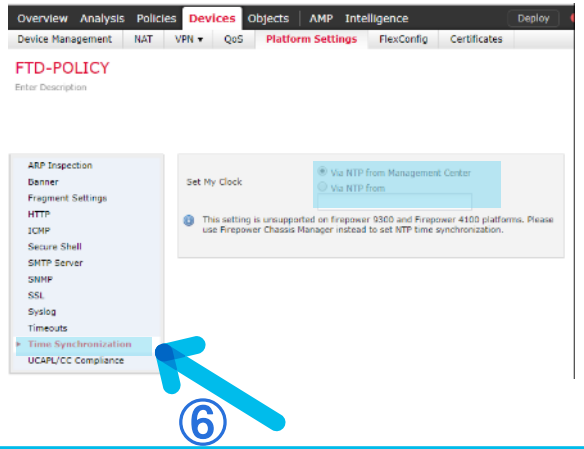
5章で実施

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

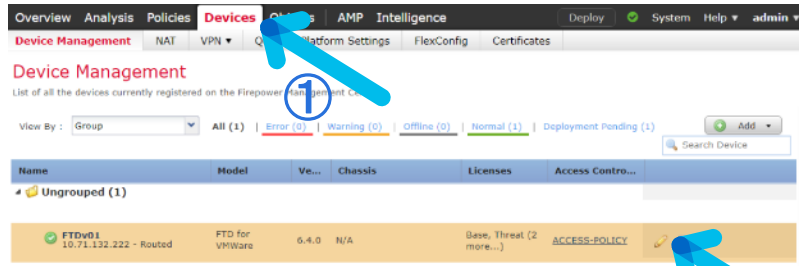
ステップ1-2：Time Synchronization

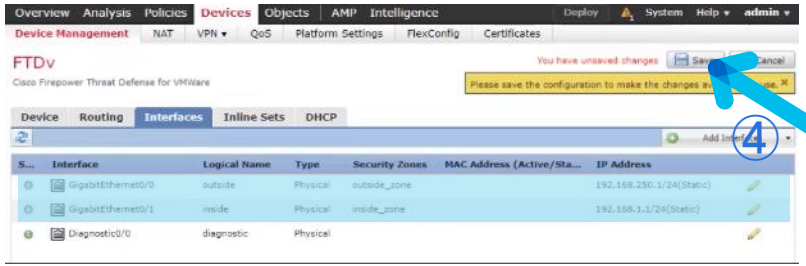
① “Deploy”を選択
② 変更された設定を確認の上、Deploy対象機器にチェックを入れる
③ “Deploy”を選択

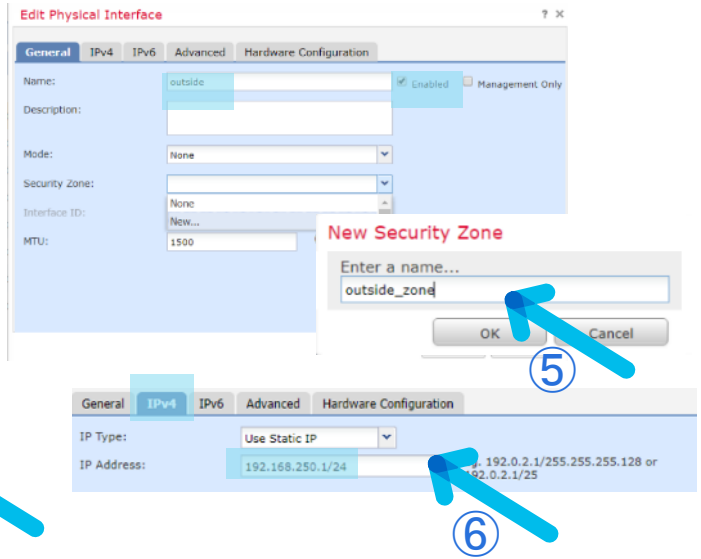
(注)FP4100,FP9300のNTPはFXOS側の設定に従う。ただし、ここで設定しても無視されるだけで問題は無い。

ステップ2：Interface設定

- FTDのRouted Interfaceを設定





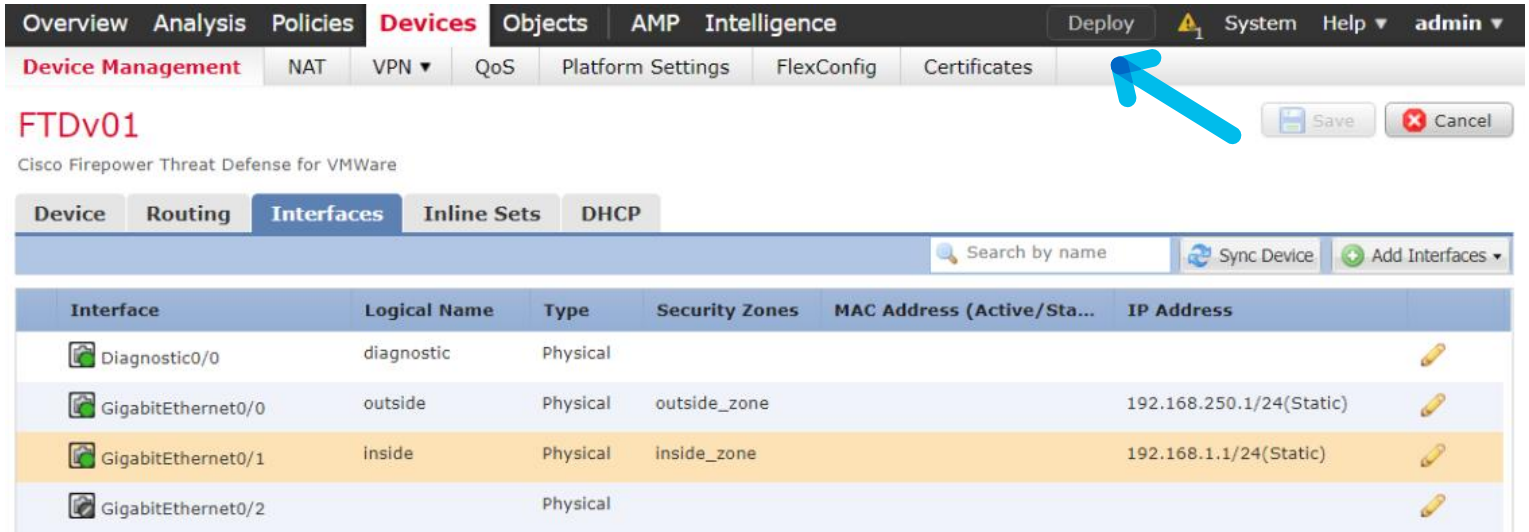


① Devicesを選択し Device Managementを選択
② 鉛筆マークを選択
③ G0/0の鉛筆マークを選択
④ 物理インターフェスの名前を入力し、Enabledにチェック
⑤ Security Zoneの名前を入力しOK
⑥ IPv4のタブに移動しIPv4アドレスを割り振ってOKをクリック
⑦ ※同様にしてGi0/1をInsideインタフェースとして設定し、saveする

Security Zone = Interfaceのグループ

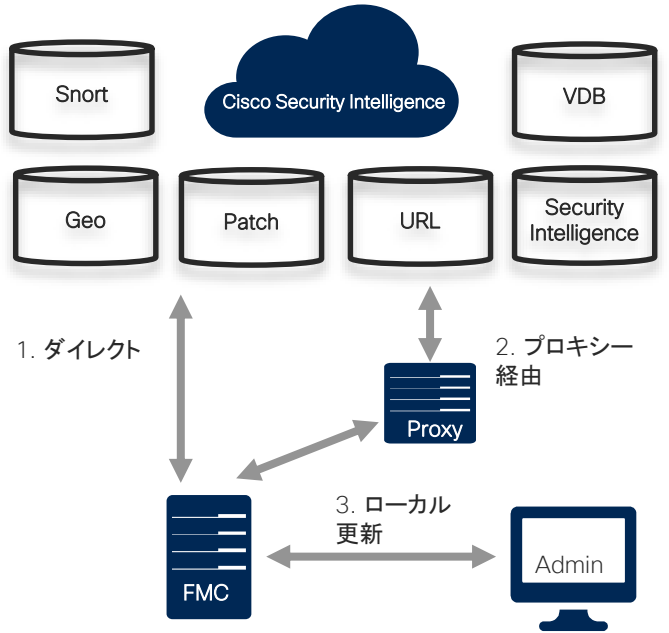
ステップ2：Interface設定

- Deployを押し設定を反映



3. シグネチャ及び各種DBの更新

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

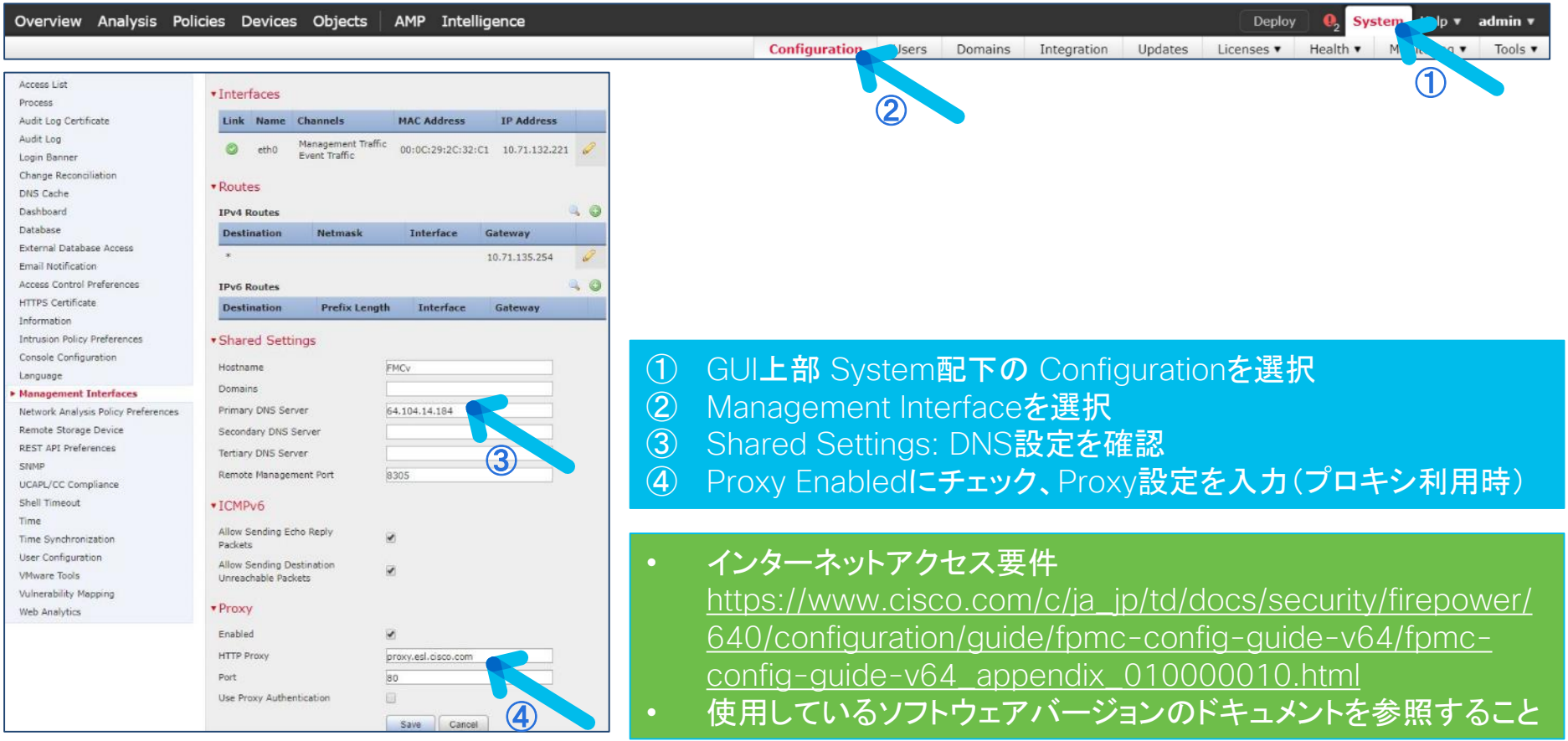
更新パッケージおよび内容一覧

	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)	Cisco_Firepower_Mgmt_Center_Patch-6.4.0.8-28.sh.REL.tar	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	Cisco_Firepower_SRU-2020-04-24-001-vrt.sh.REL.tar	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	Cisco_Firepower_GEODB_Update-2020-04-13-002.sh.REL.tar	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	Cisco_VDB_Fingerprint_Database-4.5.0-333.sh.REL.tar	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

※Software 6.3以前のファイル名の命名規則は、6.4以降とは異なる (Sourcefire_xxxという命名規則になっている)

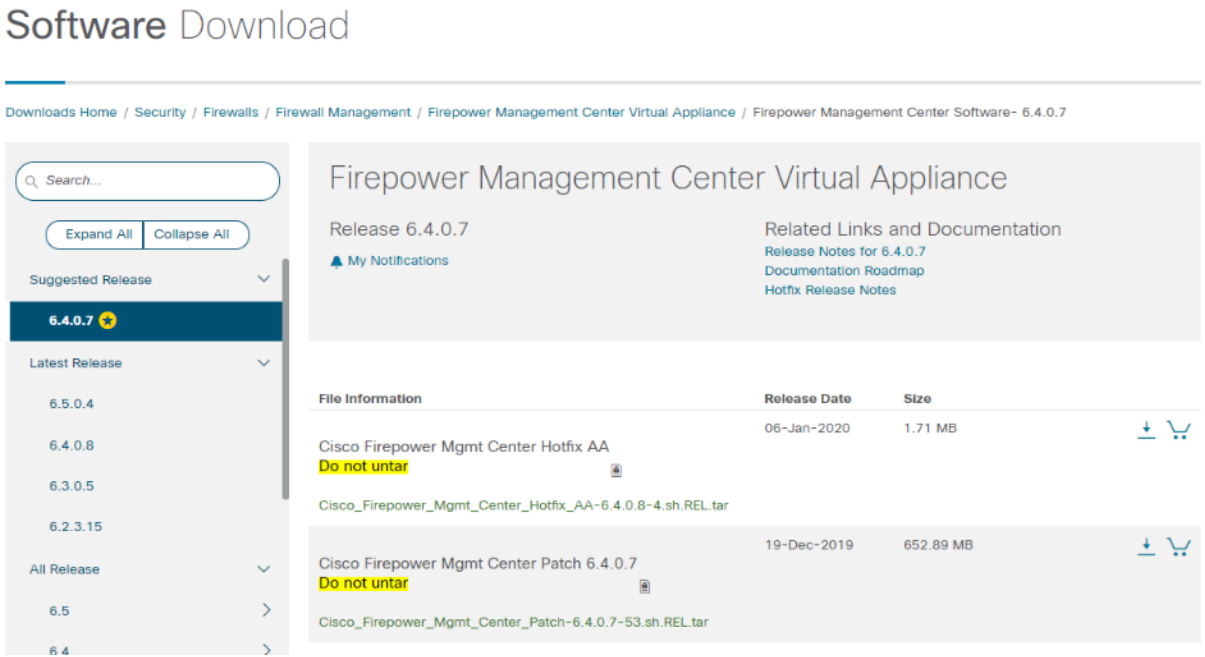
クラウド接続方法の確認



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）

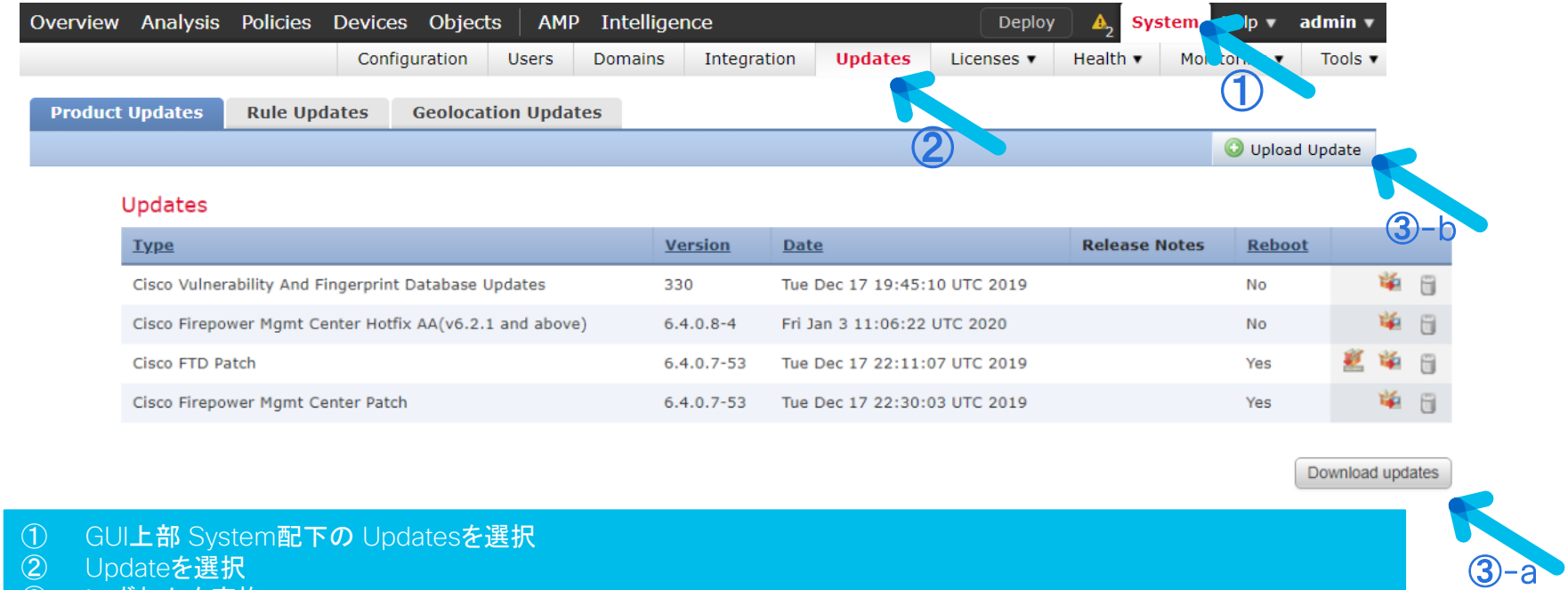
- インターネットアクセス要件
  https://www.cisco.com/c/ja_jp/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/fpmc-config-guide-v64_appendix_010000010.html
- 使用しているソフトウェアバージョンのドキュメントを参照すること

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



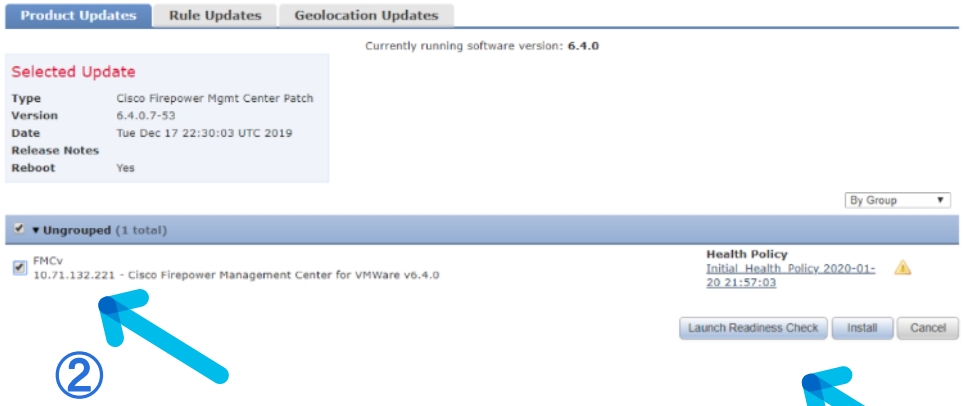
① GUI上部 System配下の Updatesを選択
② Updateを選択
③ いずれかを実施
  a. ダイレクト/Proxy経由のクラウド更新：Product Updates下のDownloaded Updatesを選択。Patch, VDBに更新がある場合、更新可能なファイルが表示される
  b. ローカル更新：Upload Updateを選択。VDBもしくは FMC/FTD Patchをアップロード

- ③-a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

Updates

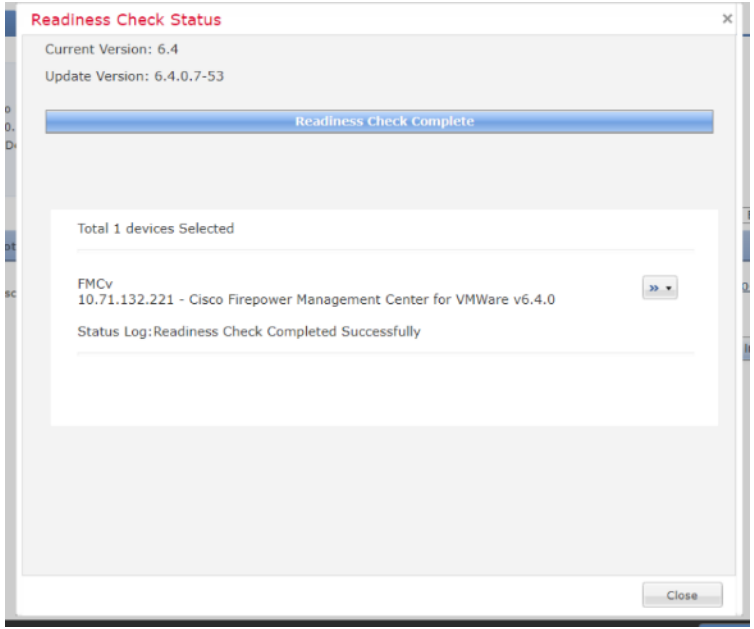
Type	Version	Date	Release Notes	Reboot	
Cisco Vulnerability And Fingerprint Database Updates	330	Tue Dec 17 19:45:10 UTC 2019		No	
Cisco Firepower Mgmt Center Hotfix AA(v6.2.1 and above)	6.4.0.8-4	Fri Jan 3 11:06:22 UTC 2020		No	
Cisco FTD Patch	6.4.0.7-53	Tue Dec 17 22:11:07 UTC 2019		Yes	
Cisco Firepower Mgmt Center Patch	6.4.0.7-53	Tue Dec 17 22:30:03 UTC 2019		Yes	

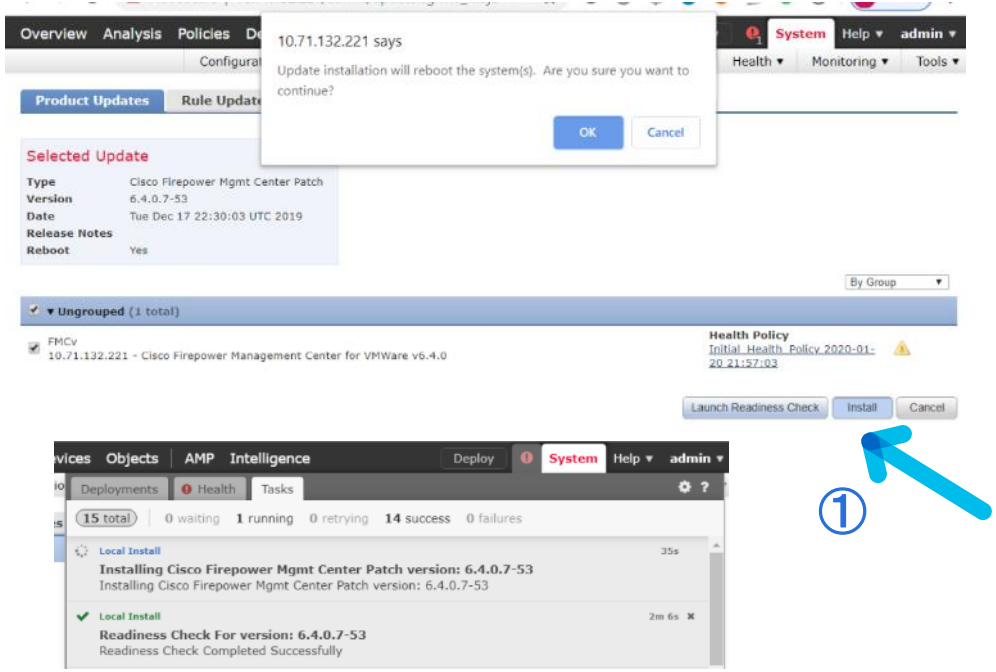


① Updates欄にある マークを選択
② 更新ファイルをインストールする対象デバイスを選択
③ Launch Readiness Checkを選択

- 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

VDB/Patch ワンタイム更新～インストール





① Readiness Check実施後、Installを選択

VDB/Patch ワンタイム更新～インストール

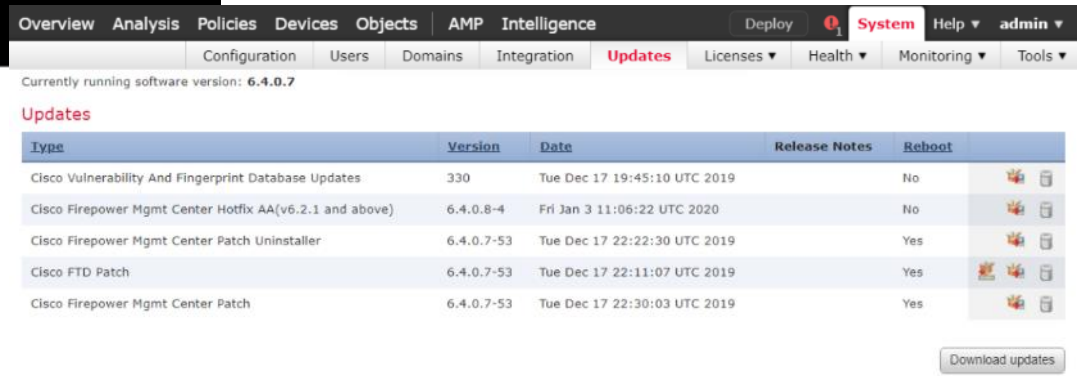
参考: シスココミュニティ FMC FTD 6.x : パッチインストール履歴の確認方法
https://community.cisco.com/t5/-/-/ta-p/3166723

①

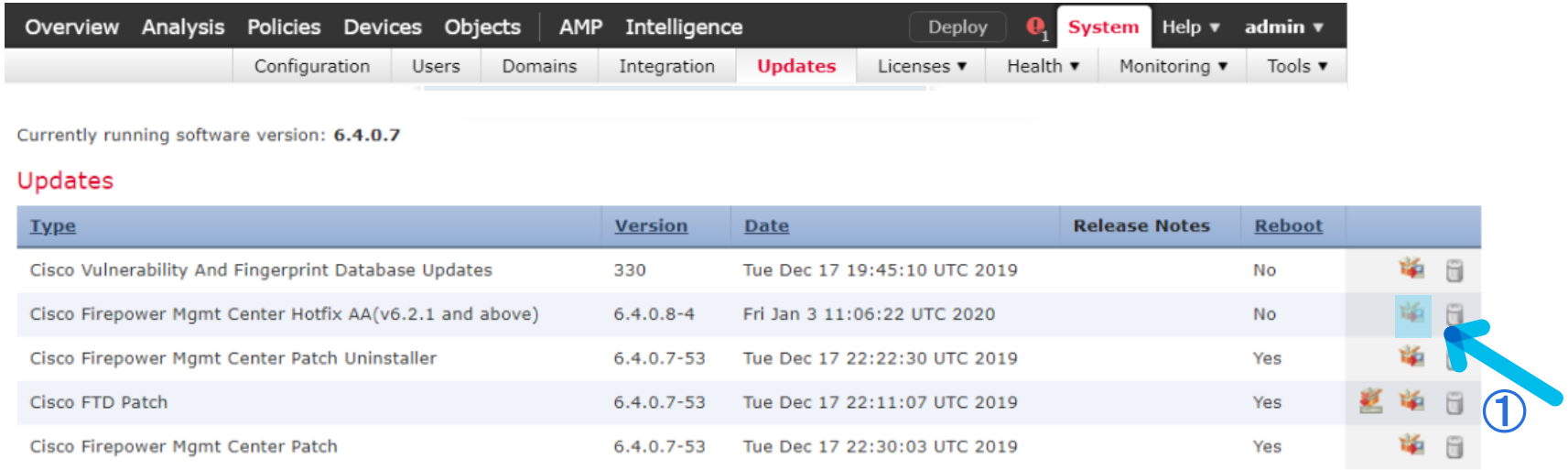
```
FMCv login: admin
Password:
Last failed login: Fri Jan 24 13:56:44 UTC 2020 on tty1
There was 1 failed login attempt since the last successful login.
Last login: Fri Jan 24 13:56:50 UTC 2020 on tty1

Copyright 2004-2019, 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 v6.4.0 (build 2)
Cisco Firepower Management Center for VMWare v6.4.0.7 (build 53)

admin@FMCv:~$ cat /etc/sf/patch_history
6.4.0-102
6.4.0.7-53
admin@FMCv:~$ _
```

① パッチ適用状況の確認方法 (CLI)
cat/etc/sf/patch_history
② パッチ適用状況の確認方法(GUI)

②



Hotfixの適用



① 同様の要領でHotfixをインストール

- 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

Hotfixの適用

① パッチ適用状況の確認方法 (CLI)
② パッチ適用状況の確認方法(GUI)

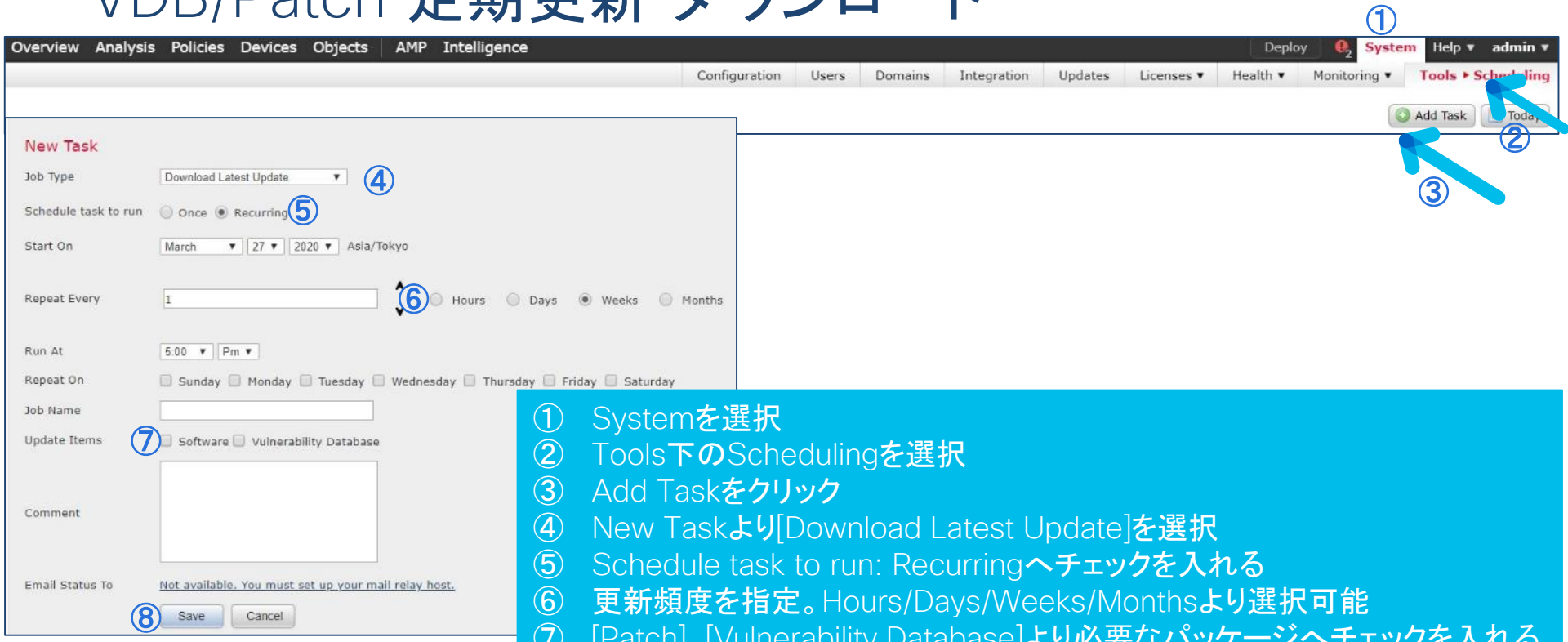
①

```
admin@FMCv:~$ cat /etc/sf/patch_history
6.4.0-102
6.4.0.7-53
Hotfix_AA-4__513438484
admin@FMCv:~$ _
```

②

Cisco Firepower Mgmt Center Hotfix AA(v6.2.1 and above)	6.4.0.8-4	Fri Jan 3 11:06:22 UTC 2020	No	
Cisco Firepower Mgmt Center Hotfix AA Uninstaller(v6.2.1 and above)	6.4.0.8-4	Fri Jan 3 11:06:12 UTC 2020	No	

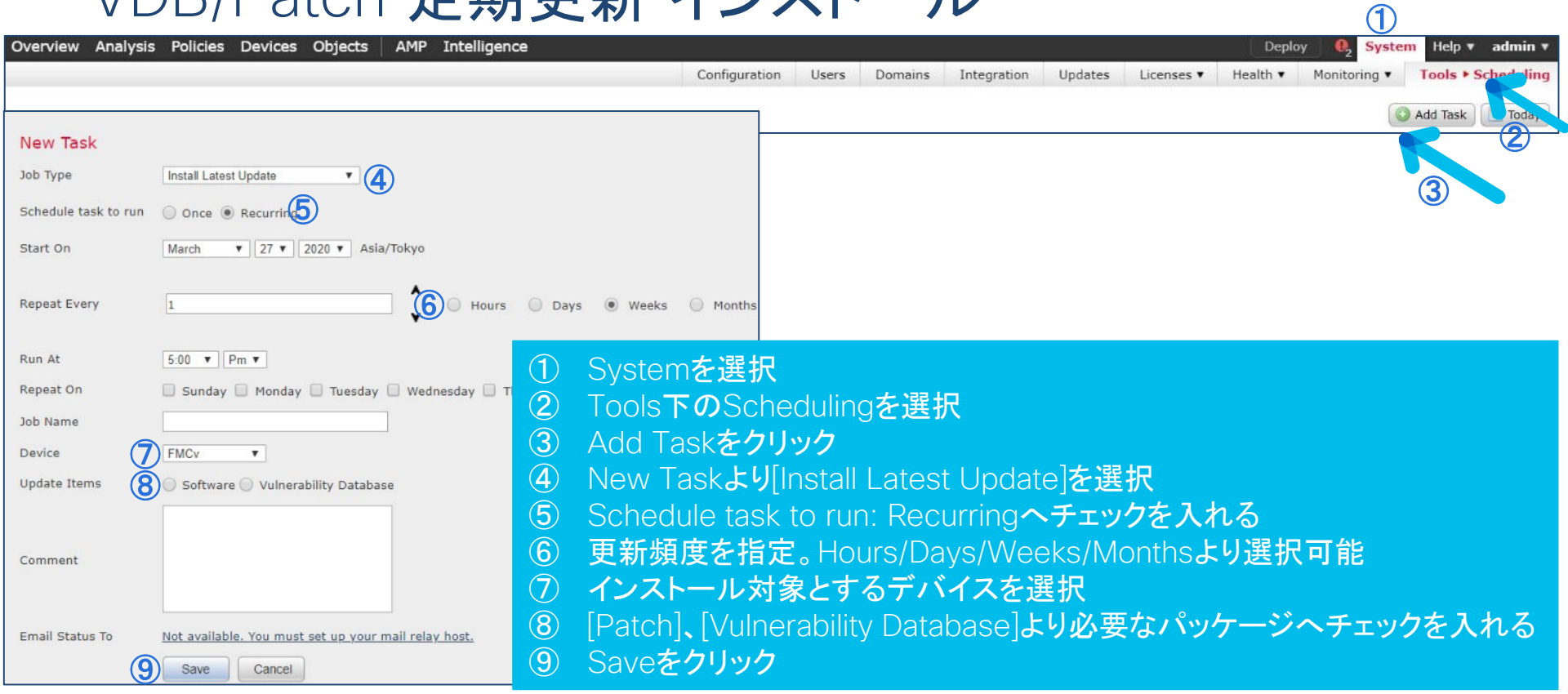
VDB/Patch 定期更新 ダウンロード



① Systemを選択
② Tools下のSchedulingを選択
③ Add Taskをクリック
④ New Taskより[Download Latest Update]を選択
⑤ Schedule task to run: Recurringへチェックを入れる
⑥ 更新頻度を指定。Hours/Days/Weeks/Monthsより選択可能
⑦ [Patch]、[Vulnerability Database]より必要なパッケージへチェックを入れる
⑧ Saveをクリック

- 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

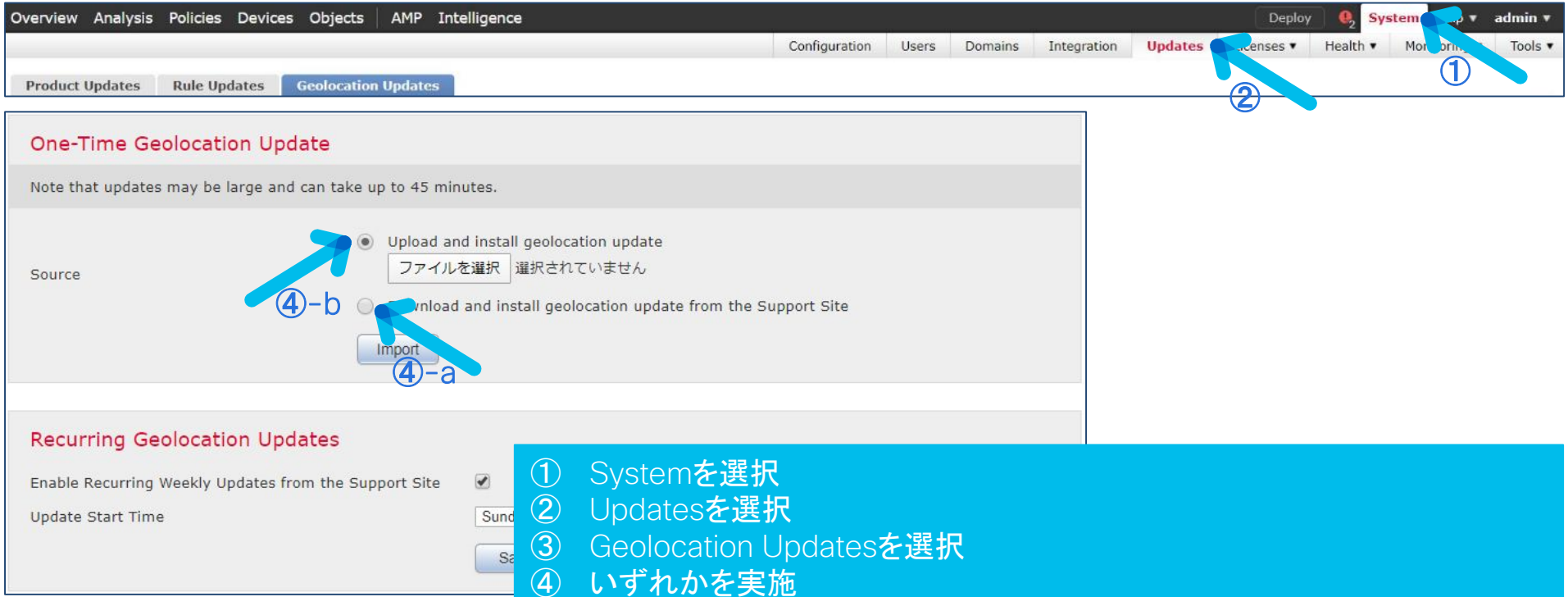
VDB/Patch 定期更新 インストール



① Systemを選択
② Tools下のSchedulingを選択
③ Add Taskをクリック
④ New Taskより[Install Latest Update]を選択
⑤ Schedule task to run: Recurringへチェックを入れる
⑥ 更新頻度を指定。Hours/Days/Weeks/Monthsより選択可能
⑦ インストール対象とするデバイスを選択
⑧ [Patch]、[Vulnerability Database]より必要なパッケージへチェックを入れる
⑨ Saveをクリック

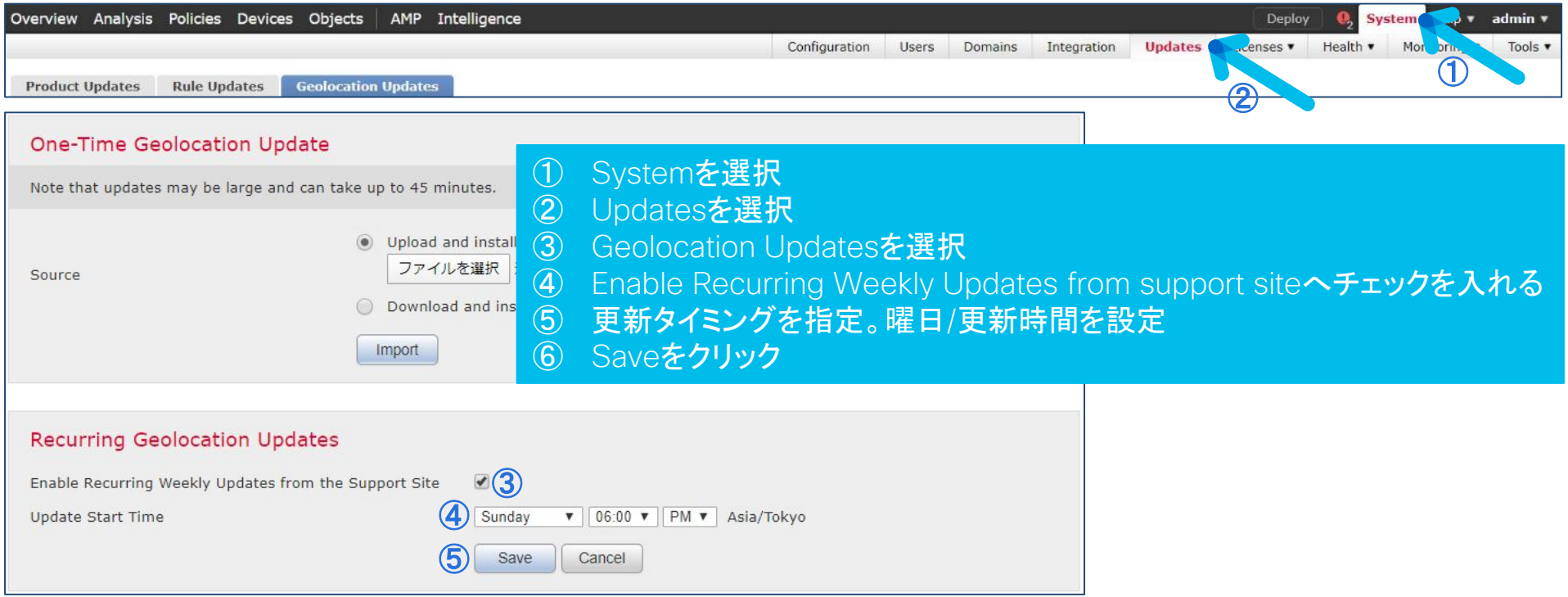
- VDB/Patchインストールは、FTDデータ通信トラフィック影響があるため実施時間に注意

GeoDB ワンタイム更新



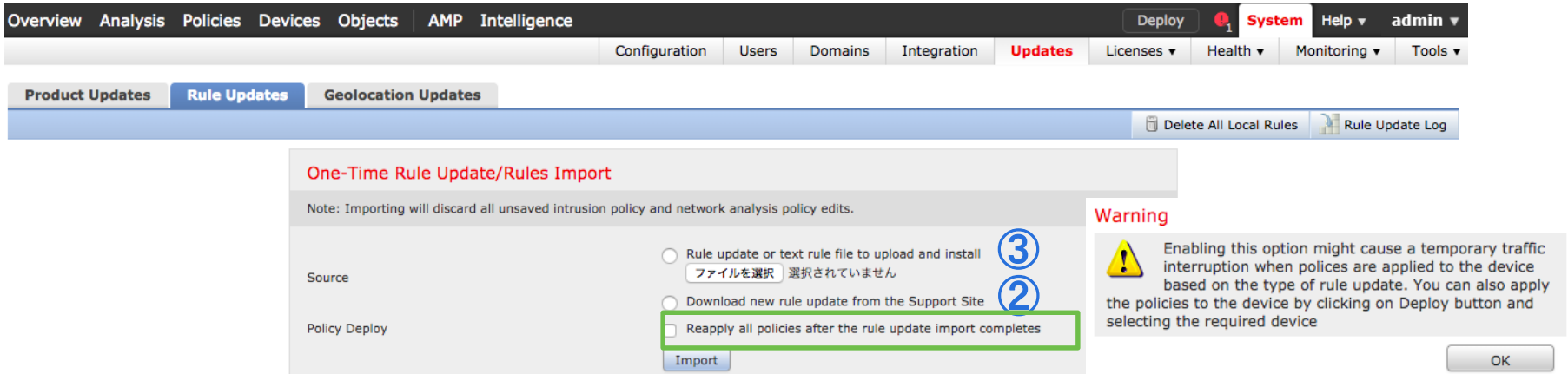
① Systemを選択
② Updatesを選択
③ Geolocation Updatesを選択
④ いずれかを実施
   a. ダイレクト/Proxy経由のクラウド更新: [Download new geolocation update from support site]を選択し、Importをクリック
   b. ローカル更新：Source: Download and install geolocation update from support siteを選択後、ファイルをアップロードして Importをクリック

GeoDB 定期更新



① Systemを選択
② Updatesを選択
③ Geolocation Updatesを選択
④ Enable Recurring Weekly Updates from support siteへチェックを入れる
⑤ 更新タイミングを指定。曜日/更新時間を設定
⑥ Saveをクリック

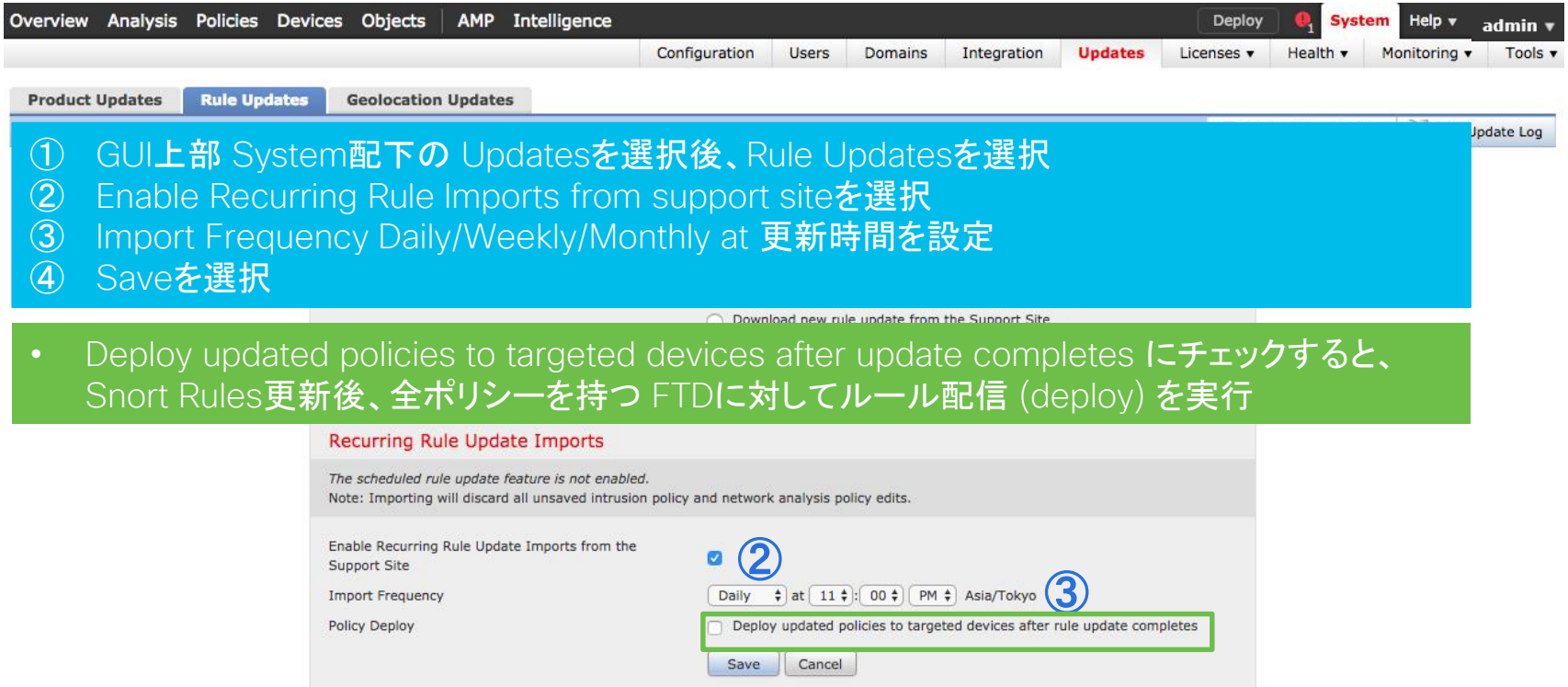
Snort Rules ワンタイム更新



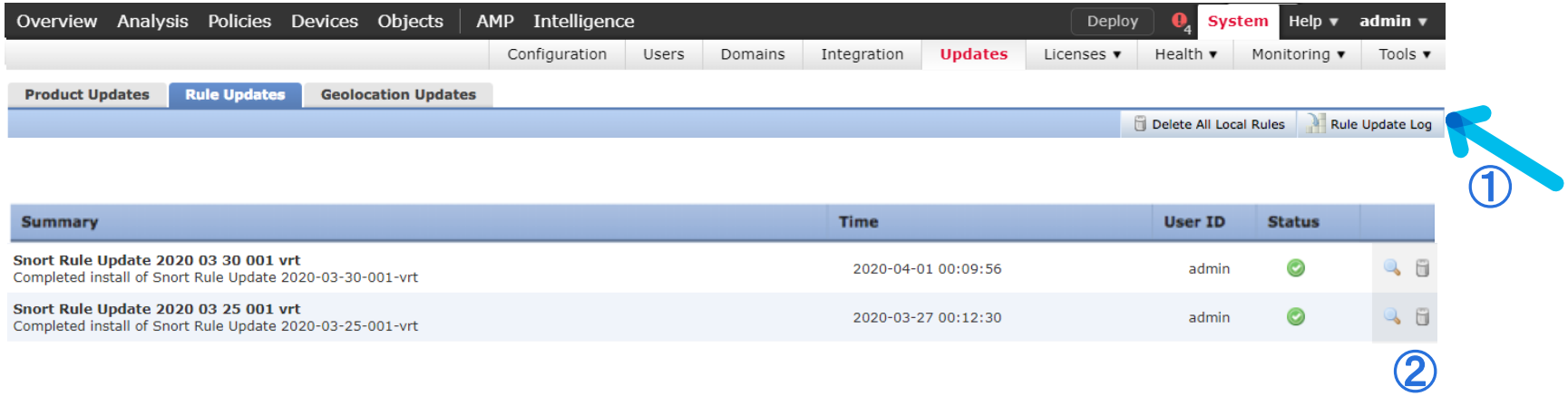
① GUI上部 System配下の Updatesを選択後、Rule Updatesを選択
② Source: Download new rule update from support siteを選択後、Importを選択 (ダイレクトもしくはProxy経由更新の場合)
③ Source: Rule Update or txt rule file to upload and installを選択後、ファイルをアップロードして Importを選択 (ローカル更新の場合)

- 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 (deploy) 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

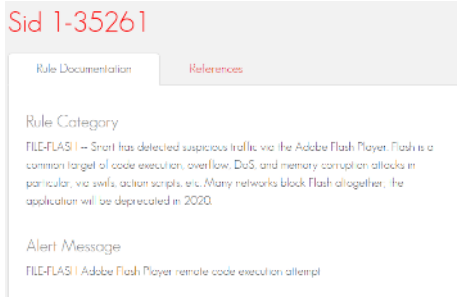


① GUI上部 System配下の Updatesを選択後、Rule Update Logを選択
② インストールされたパッケージ(-vrt)の マークを選択

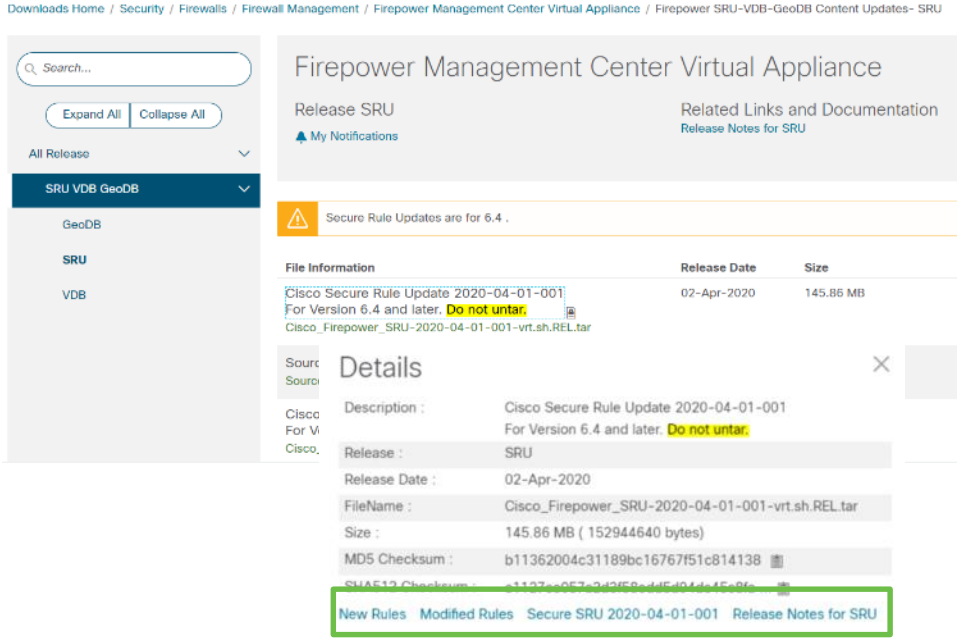
Snort Rules 更新ログ

Time	Name	Type	Action	GID	SID	Rev
2020-01-31 00:11:15	MALWARE-OTHER Win.Trojan.Ponystealer-7564561-0 download attempt	rule	new	1	52992	1
2020-01-31 00:11:15	FILE-FLASH Adobe Flash Player remote code execution attempt	rule	changed	1	35261	3
2020-01-31 00:11:15	BROWSER-IE Microsoft Internet Explorer improper copy buffer access information disclosure attempt	rule	new	1	52985	1
2020-01-31 00:11:15	BROWSER-IE Microsoft Edge memory corruption attempt	rule	changed	1	48770	2

- 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



Cisco Talos Update for FireSIGHT Management Center

Date: 2020-04-02

This SRU number: 2020-04-01-001
Previous SRU number: 2020-03-30-001
Applies to:

- 3D Sensor versions: 5.x / 6.x
- Cisco FireSIGHT Management Center versions: 5.x / 6.x

This SEU number: 2145
Previous SEU: 2144
Applies to:

- 3D Sensor Versions: 4.10
- Cisco FireSIGHT Management Center versions: 4.10

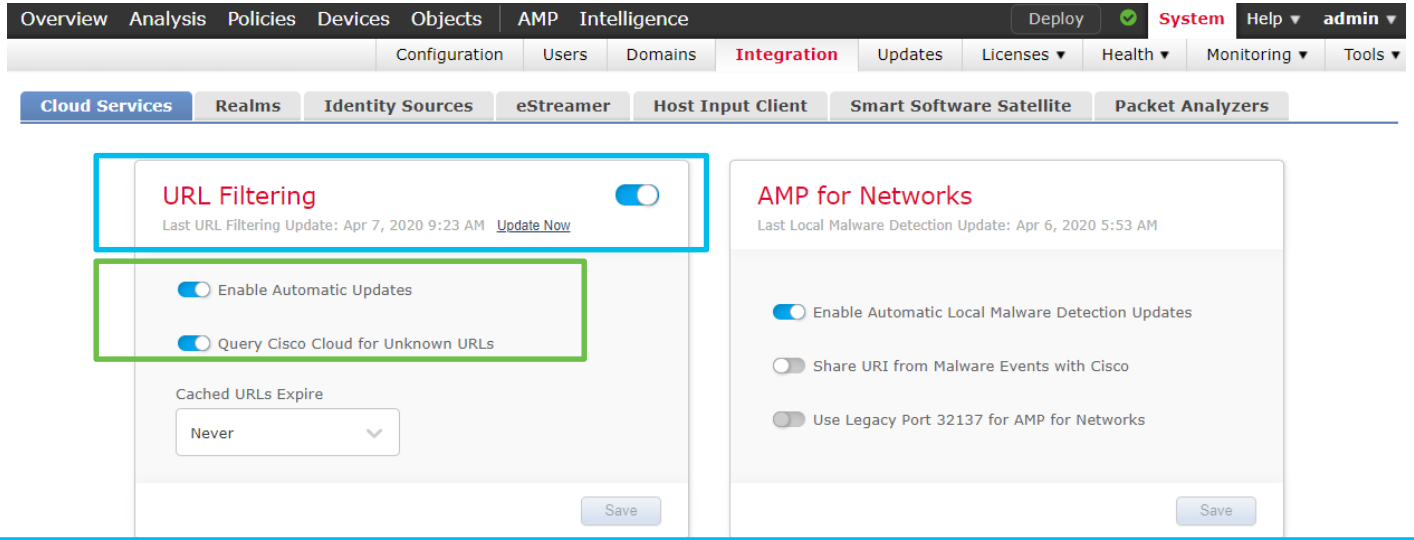
This is the complete list of rules added in SRU 2020-04-01-001 and SEU 2145.
The format of the file is:
GID - SID - Rule Group - Rule Message - Policy State
The Policy State refers to each default Cisco Talos policy, Connectivity, Balanced, Security, and Maximum Detection.
The default passive policy state is the same as the Balanced policy state with the exception of alert being used instead of drop.
Note: Unless stated explicitly, the rules are for the series of products listed above.

New Rules:

			High Priority	Policy State			
GID	SID	Rule Group	Rule Message	Con.	Bal.	Sec.	Max.
1	53525	MALWARE-OTHER	Win.Dropper.Tdss-7643790-0 download attempt	off	off	drop	drop
1	53526	MALWARE-OTHER	Win.Dropper.Tdss-7643790-0 download attempt	off	off	drop	drop
1	53527	MALWARE-OTHER	Unix.Exploit.Lotoor-7643871-0 download attempt	off	off	drop	drop
1	53528	MALWARE-OTHER	Unix.Exploit.Lotoor-7643871-0 download attempt	off	off	drop	drop
1	53529	MALWARE-OTHER	Win.Malware.Winspy-7644935-0 download attempt	off	off	drop	drop
1	53530	MALWARE-OTHER	Win.Malware.Winspy-7644935-0 download attempt	off	off	drop	drop
3	53531	OS-WINDOWS	TRUFFLEHUNTER TALOS-2020-1033 attack attempt	off	off	drop	drop
3	53532	OS-WINDOWS	TRUFFLEHUNTER TALOS-2020-1033 attack attempt	off	off	drop	drop
1	53533	BROWSER-CHROME	Google Chrome desktopMediaPickerController use after free attempt	off	off	drop	drop
1	53534	BROWSER-CHROME	Google Chrome desktopMediaPickerController use after free attempt	off	off	drop	drop
3	53535	FILE-OTHER	TRUFFLEHUNTER TALOS-2020-1035 attack attempt	off	off	drop	drop
3	53536	FILE-OTHER	TRUFFLEHUNTER TALOS-2020-1035 attack attempt	off	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

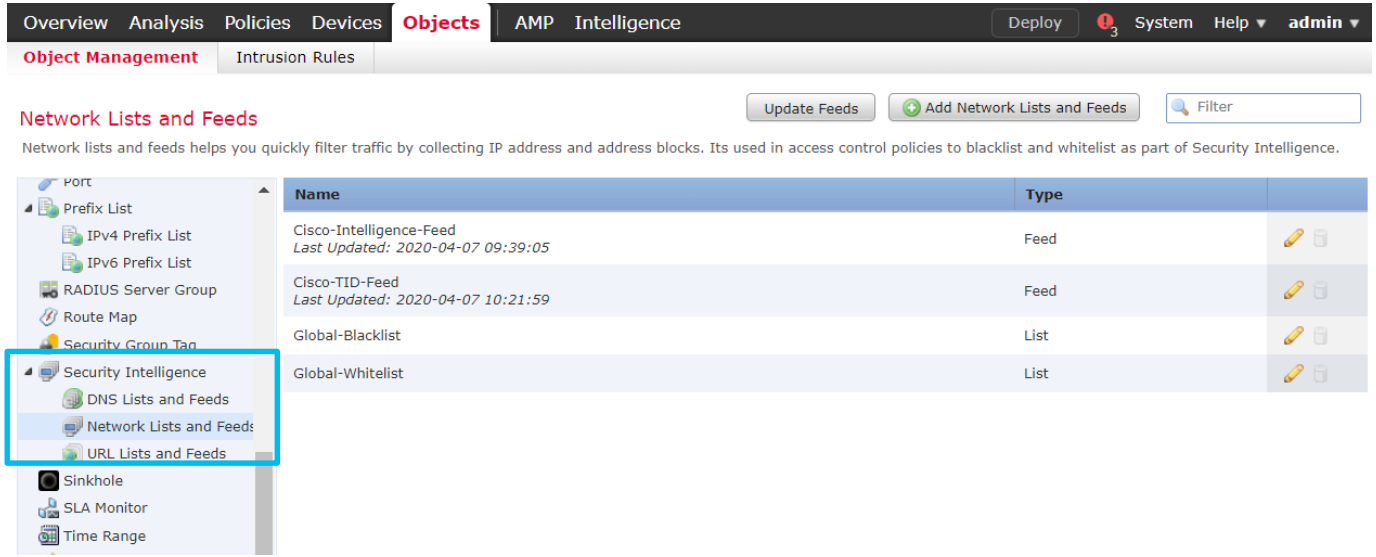
URL Filtering ワンタイム・定期更新・照会設定



① GUI上部 System配下の Integrationを選択後、Cloud Servicesを選択
② URL Filtering: URL Filtering Licenseを適用すると自動で有効化される。必要に応じて設定し、Saveを選択

- Enable Automatic Update: 30分ごとにアップデートを確認する (定期更新・ダイレクトもしくはProxy経由更新のみ)
- Query Cisco Cloud for Unknown URLs: URLカテゴリやレピュテーションがローカルで確認できない場合に、クラウドへ照会する。プライバシーの問題等でこの機能を利用したくない場合は無効にする。
- 通信要件はConfiguration GuideのChapter: Security, Internet Access, and Communication Portsに記載
  https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html

Security Intelligence 定期更新・スケジューリング変更

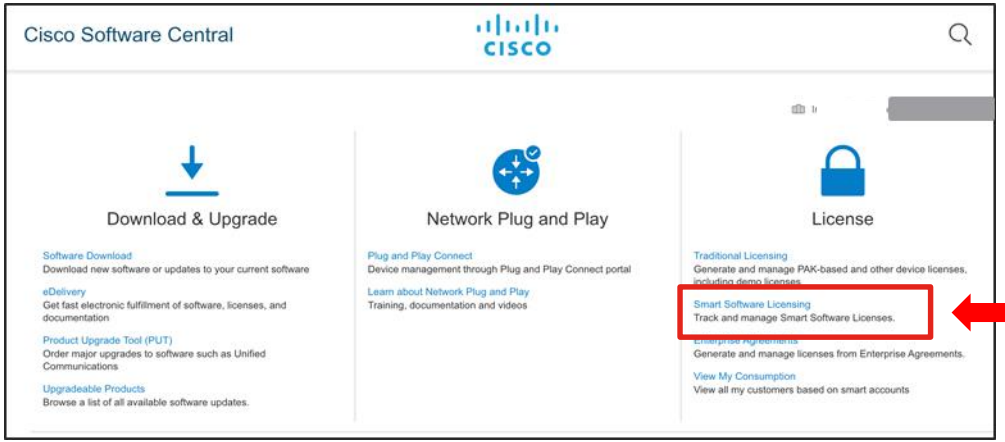


① GUI上部 Objects配下の Object Managementを選択
② Security Intelligence内の Network Lists and Feed または DNS Lists and Feedを選択

- 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

4. スマートライセンスの適用

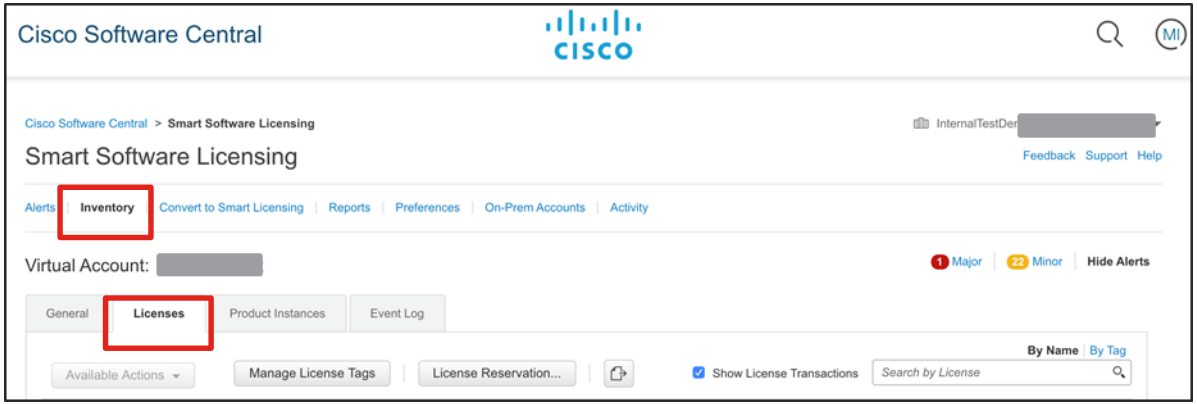
ステップ 1-1: CSSMにてライセンス確認



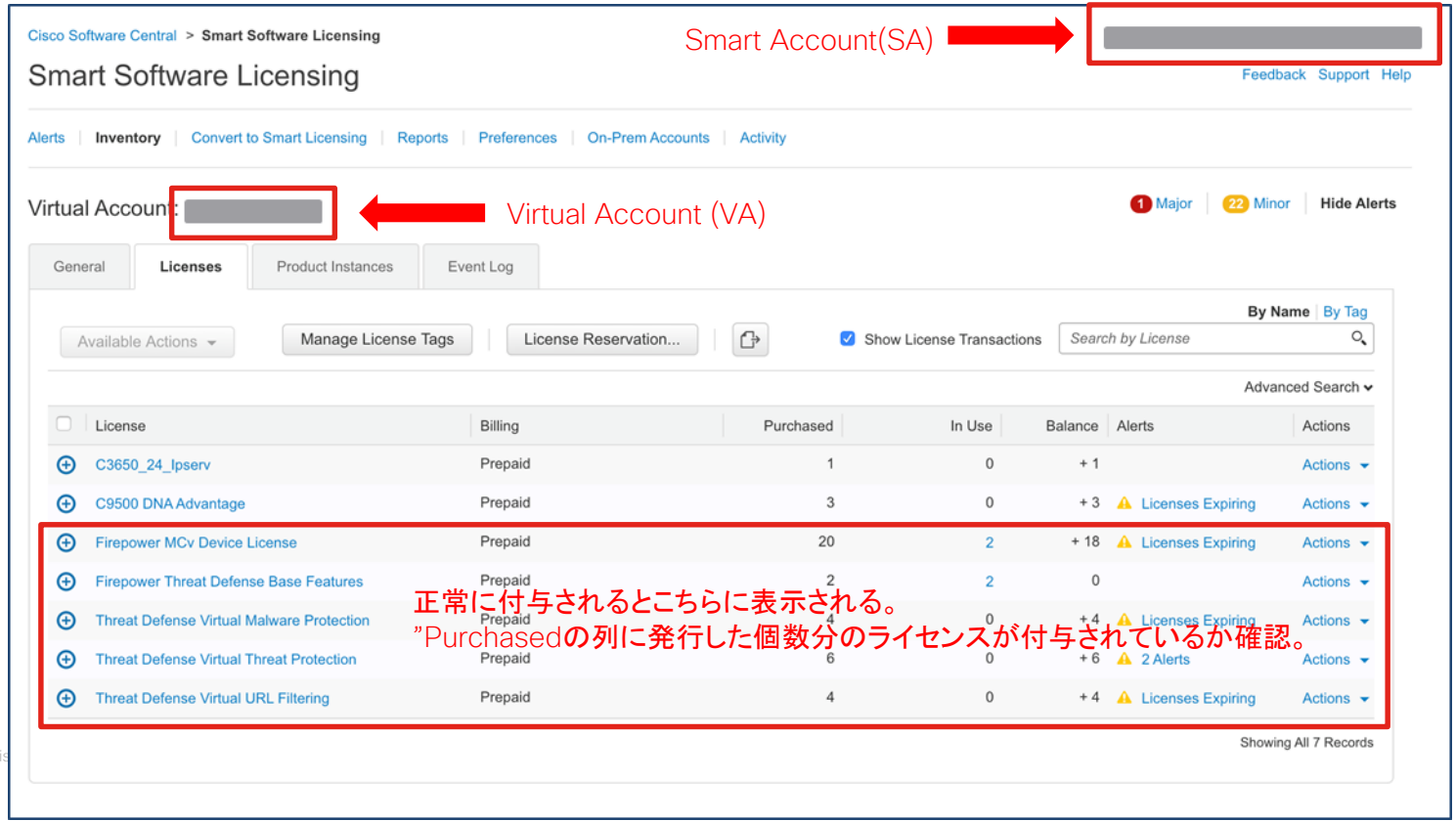
CSSM: Cisco Smart Software Manager

https://software.cisco.com/

クリック

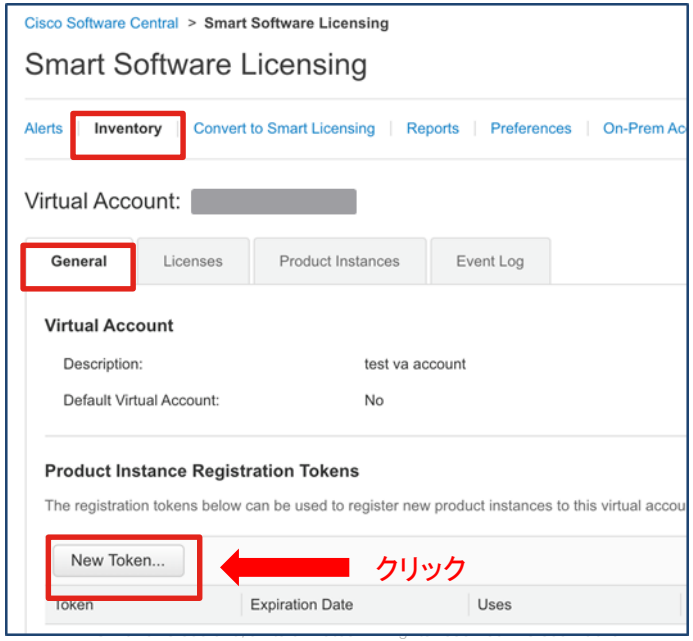


ステップ 1-2: CSSMにてライセンス確認

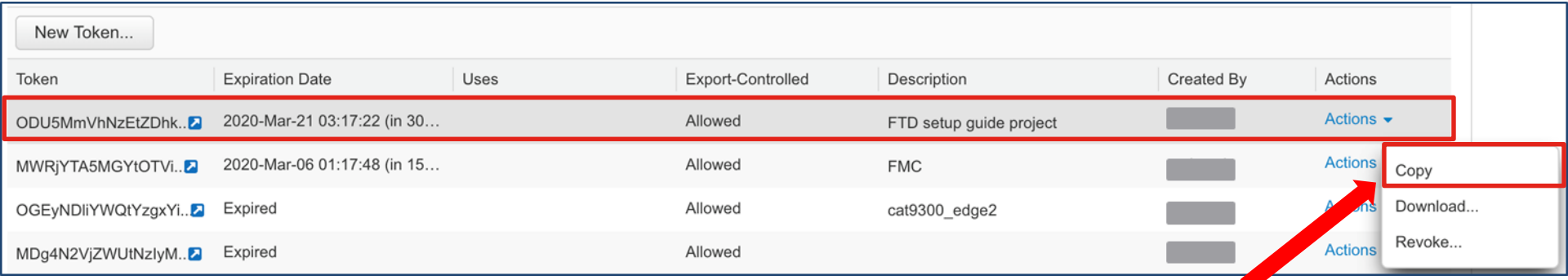


ステップ 1-3: Registration Token発行

機器登録の流れ:
①CSSMでRegistration Token発行
②発行したTokenを機器へ投入
③Tokenに記載されているSA(VA)に登録処理が走る
④VAに該当ライセンスがあれば"In Use"にカウントされる。なければ"-1"となり機材側は"out of compliance"となる



ステップ 1-4: Registration Token発行



※最新のTokenは一番上に表示される。

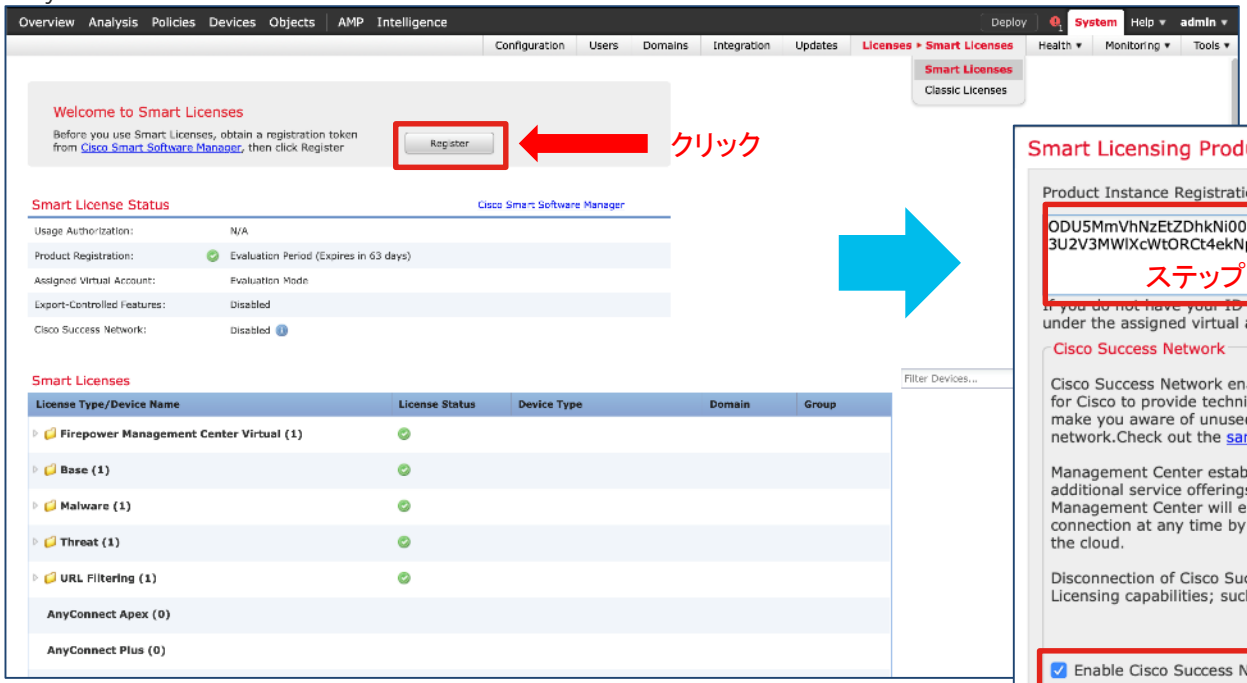
Actionsのプルダウンから
Copyをクリック

ステップ 1-5: FMCのSL登録

※FTDをFMC管理とする場合、FTDで利用するライセンスはFMCにて管理される。

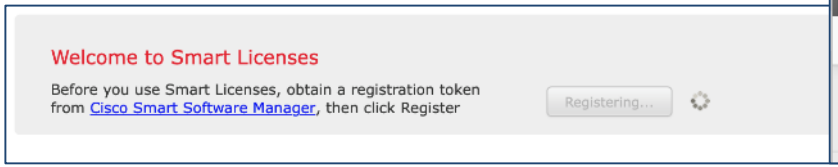
System > Licenses > Smart Licenses

※Cisco Success Network: FMC の利用状況をシスコに共有する仕組み

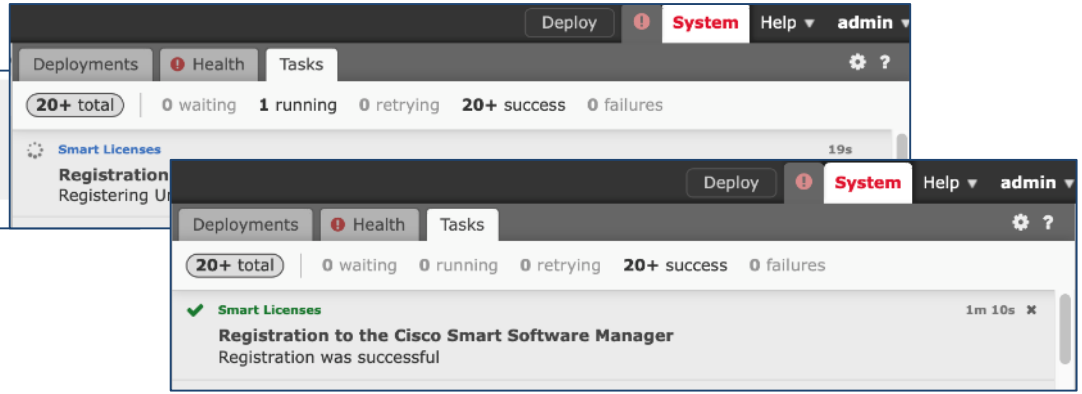


ステップ 1-6: FMCのSL登録

登録処理中の画面



Tasksでも状況確認が可能

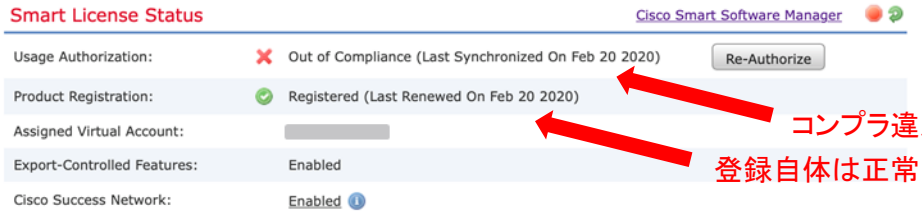


使用状況のステータス。必要なライセンスを保有していればAuthorizedとなる。

FMCで管理している製品が正常にCSSM側に登録されるとRegisteredとなる。

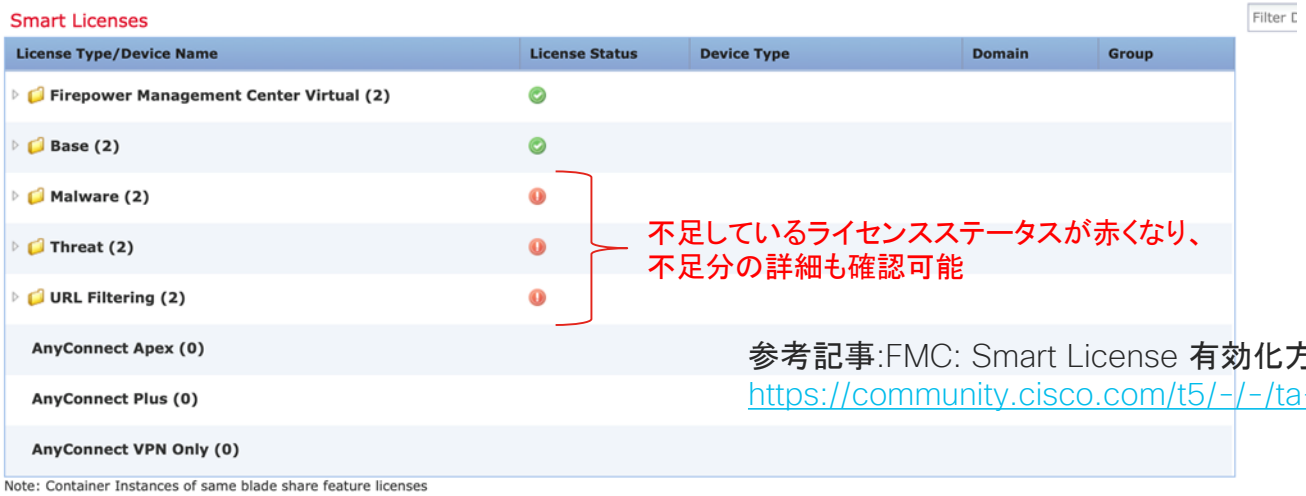
参考: FMCのSL登録(ライセンス不足のケース)

※FMCとCSSMで正常に通信は出来て登録はされたが、必要ライセンスを保持していない状態の画面



コンプラ違反の表示。

登録自体は正常



不足しているライセンスステータスが赤くなり、
不足分の詳細も確認可能

参考記事:FMC: Smart License 有効化方法とトラブルシューティング
https://community.cisco.com/t5/-/-/ta-p/3296811

5. Routed FirewallとNetwork Discoveryの設定

FTDとFMCその他初期設定に関して

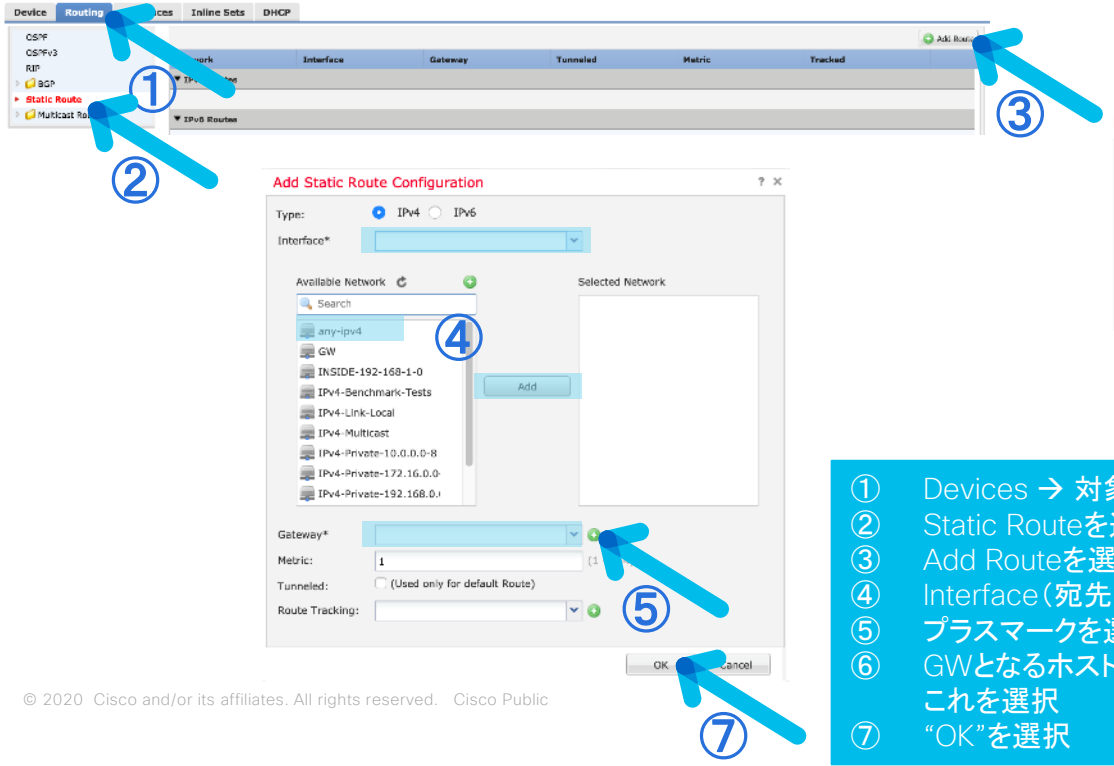
- FTDのネットワーク周りで行うべき最低限の設定を行う
  - *Time Synchronization*
  - *Interface*

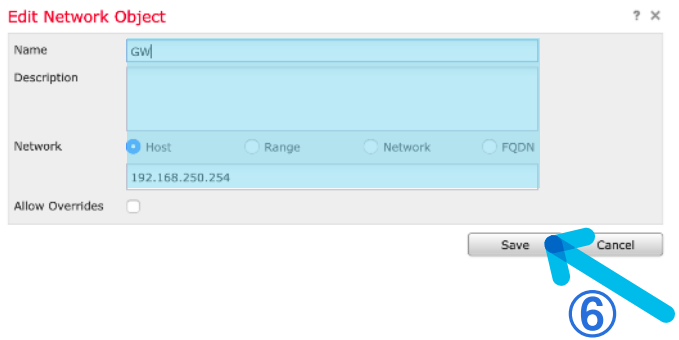
  } 2章で実施

  - Routing
  - NAT
  - Access Control Policy
  - Network Discovery Policy
  - Pre-filter

ステップ3-1：Routing

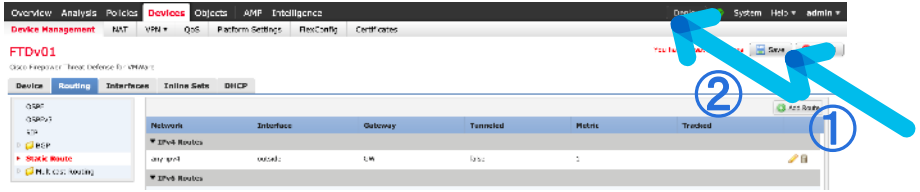
- FTDのデフォルトゲートウェイを設定。管理用のゲートウェイではなく実トラフィック用であることに注意





① Devices → 対象FTDを選択し,鉛筆マーククリック後に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 GWとなるホストとして 192.168.250.254をNW Objectとして登録し、これを選択
⑦ “OK”を選択

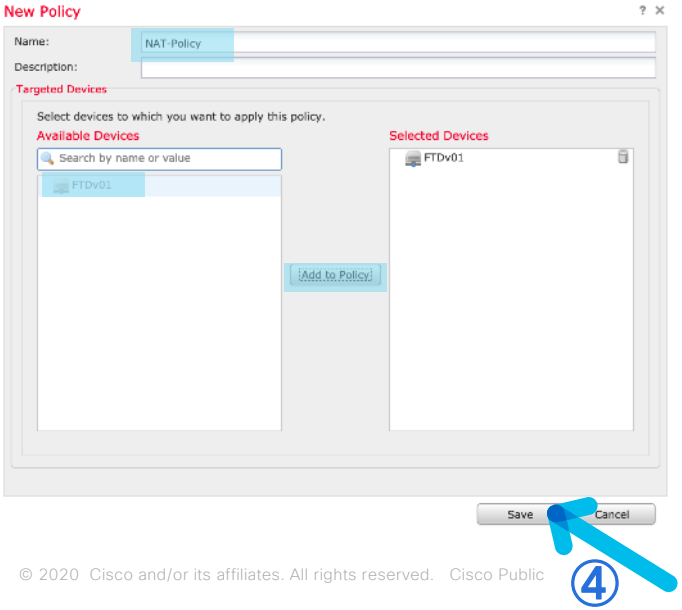
ステップ3-2：Routing

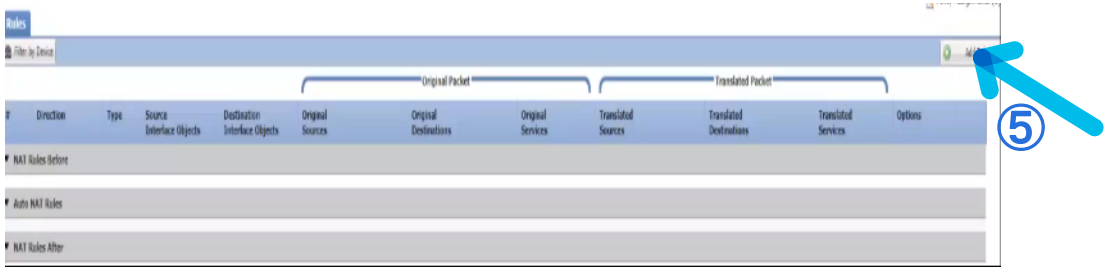


① “Save”を選択
② “Deploy”を選択
③ 変更された設定を確認の上、Deploy対象機器にチェックを入れる
④ ”Deploy”を選択

ステップ4-1：NAT

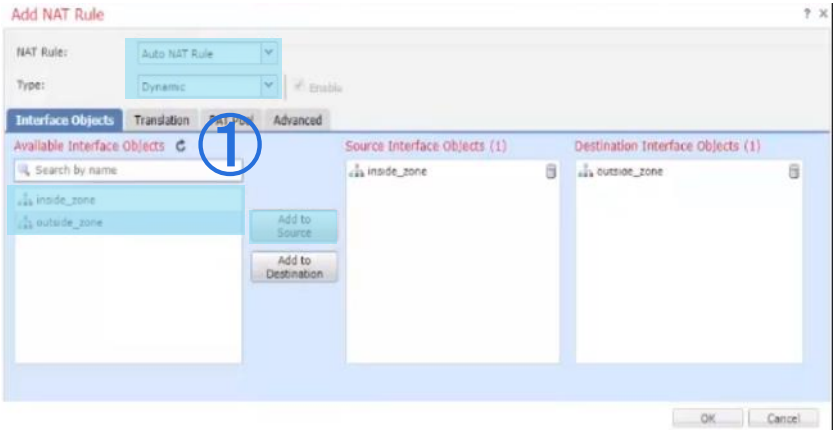
- FTDで行うNAT(PAT)を設定

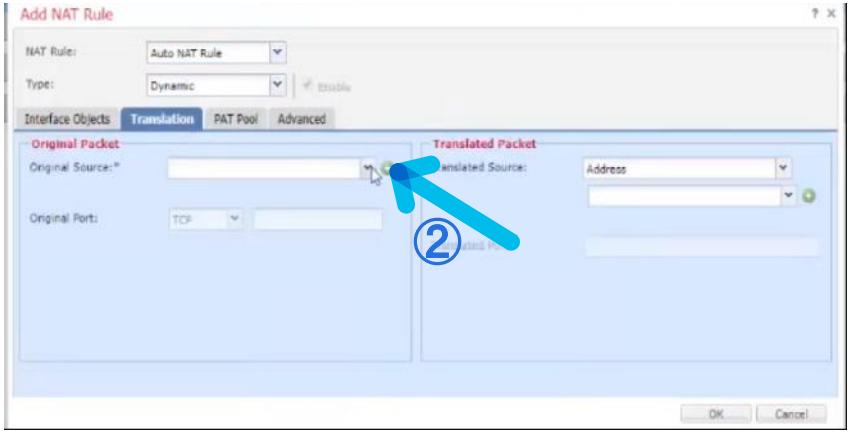




① Devicesを選択
② NATを選択
③ “Threat Defense NAT Policy”を選択
④ NAT Policyの名前、対象機器を選択し、”Save”
⑤ “Add”を選択

ステップ4-2：NAT



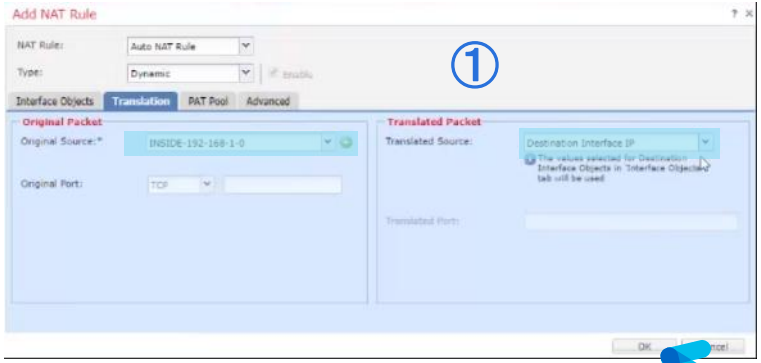


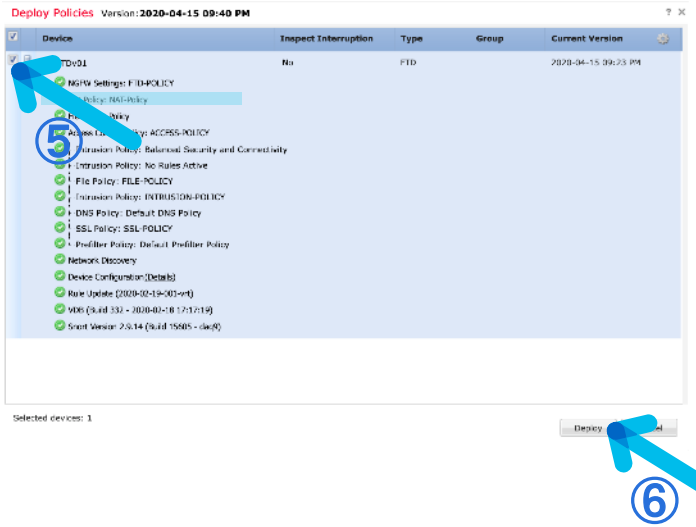
変換されるネットワークアドレス (ここでは 192.168.1.0/24) を登録

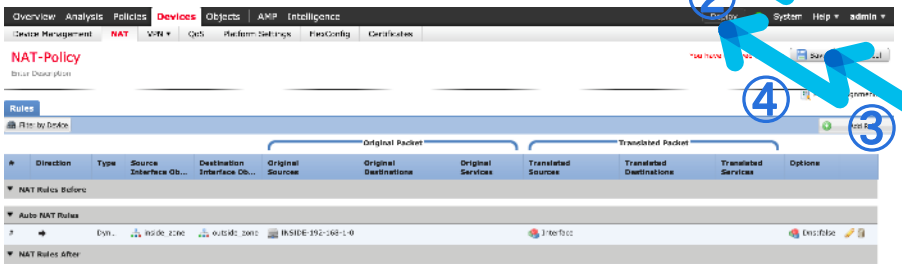
① NAT Rule、Type、SourceおよびDestinationのInterface Objectsを図のように選択
② Translation タブのプラスマークを選択
③ Network Objectとして192.168.1.0/24を作成
④ “Save”を選択

ステップ4-3：NAT

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



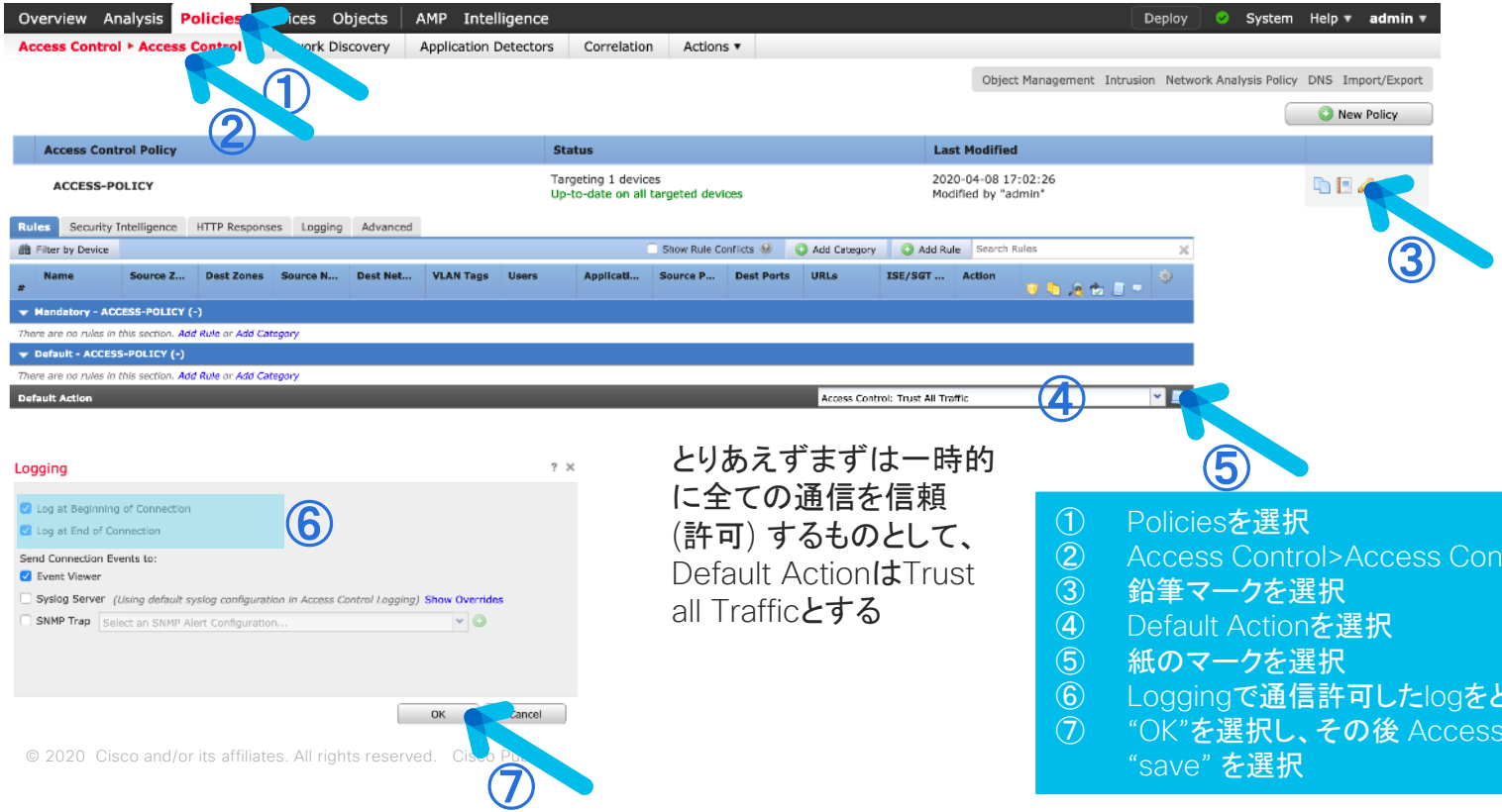




① Original Source、Destination Sourceを図のように選択
② “OK”を選択
③ “Save”を選択
④ “Deploy”を選択
⑤ 変更された設定を確認の上、Deploy対象機器にチェックを入れる
⑥ “Deploy”を選択

ステップ5-1：Access Control Policy

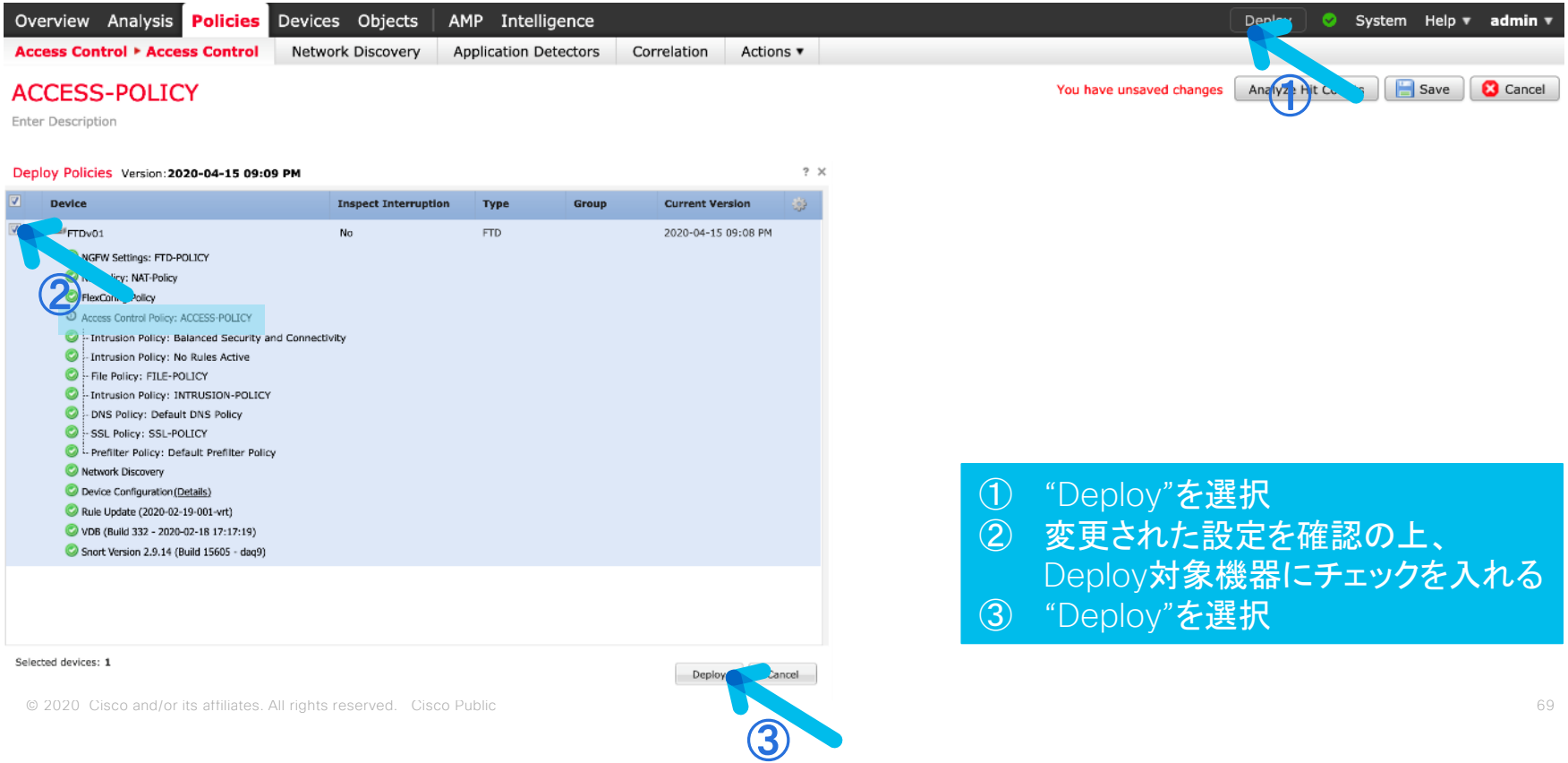
- FTDを介した通信を制御するポリシー(Access Control Policy)を修正



とりあえずまずは一時的に全ての通信を信頼(許可)するものとして、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”を選択し、その後 Access Control Policyで“save” を選択

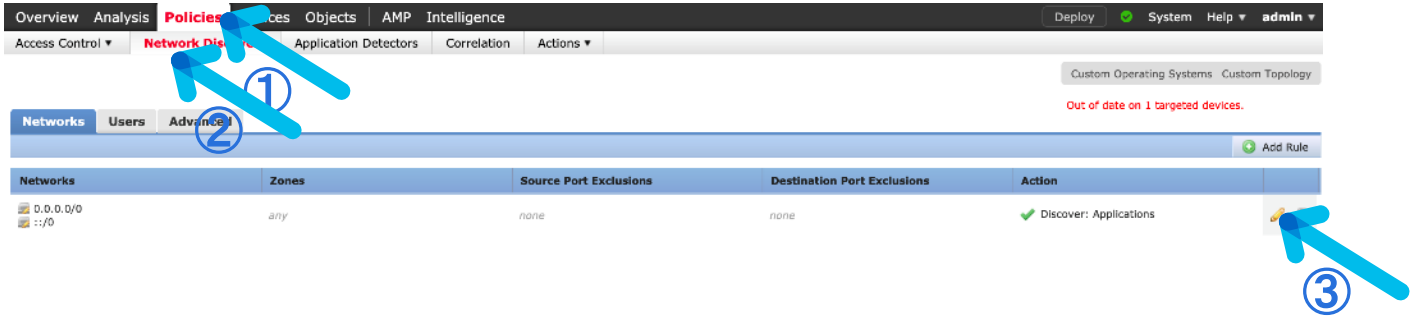
ステップ5-2：Access Control Policy



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

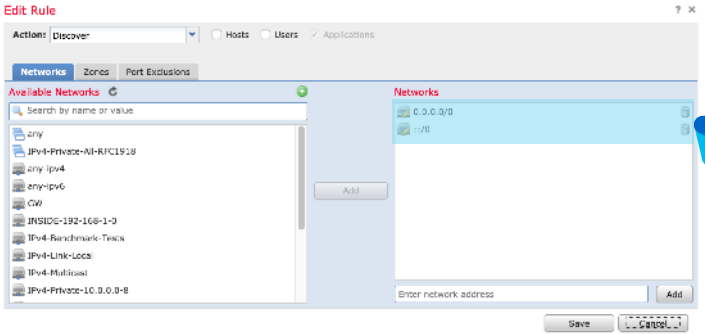
ステップ6-1：Network Discovery Policy

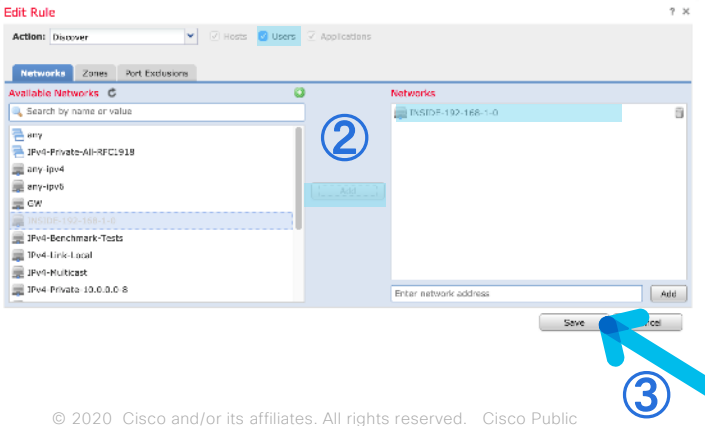
- Network Discovery Policyとは
  - 指定されたネットワーク内で、どのホスト、OS、アプリケーション等が存在するかを監視し、FMCで記憶していくためのポリシー
  - このポリシーでは監視する範囲を決め、その設定を有効にする

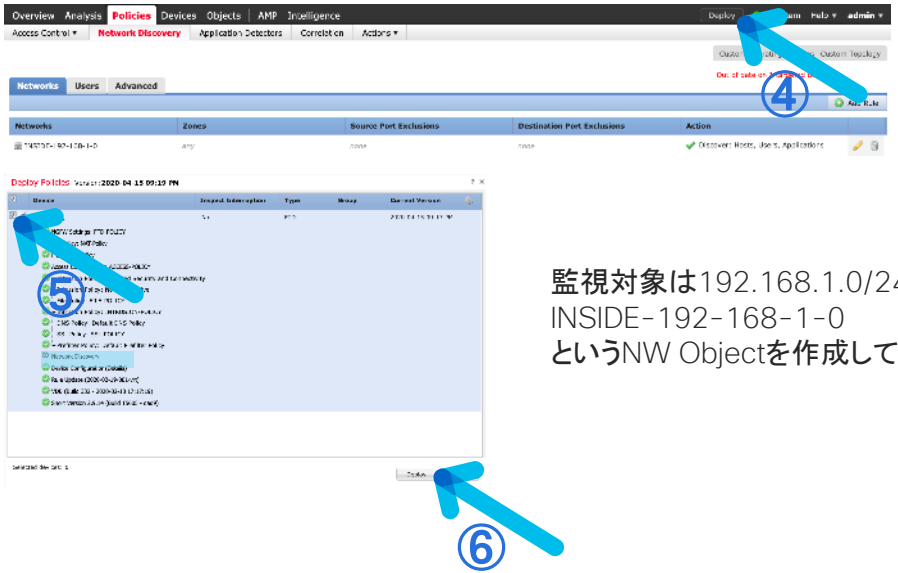


① Policiesを選択
② Network Discoveryを選択
③ 鉛筆マークを選択

ステップ6-2：Network Discovery Policy





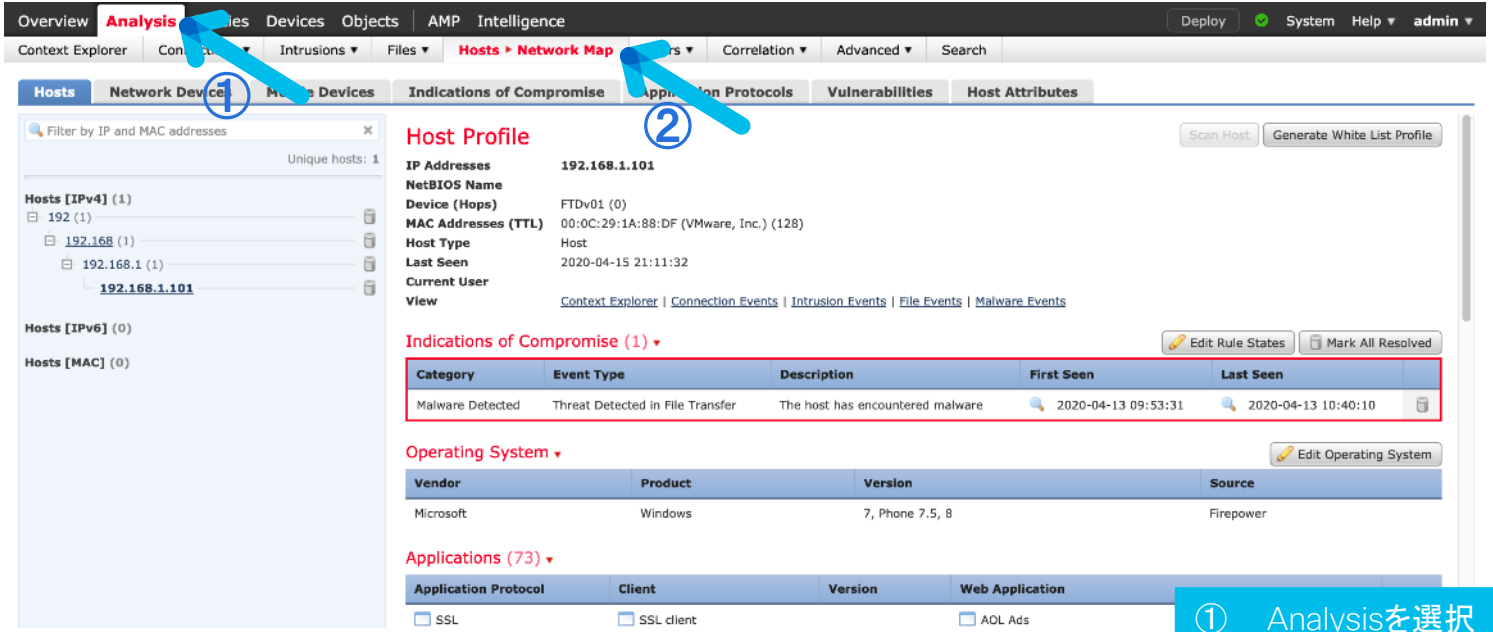


監視対象は192.168.1.0/24として、
INSIDE-192-168-1-0
というNW Objectを作成しておく

① ゴミ箱マークを選択し、登録済みのネットワークを削除
② Usersにチェックを入れ、監視対象ネットワークを”Add”ボタンで追加する（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

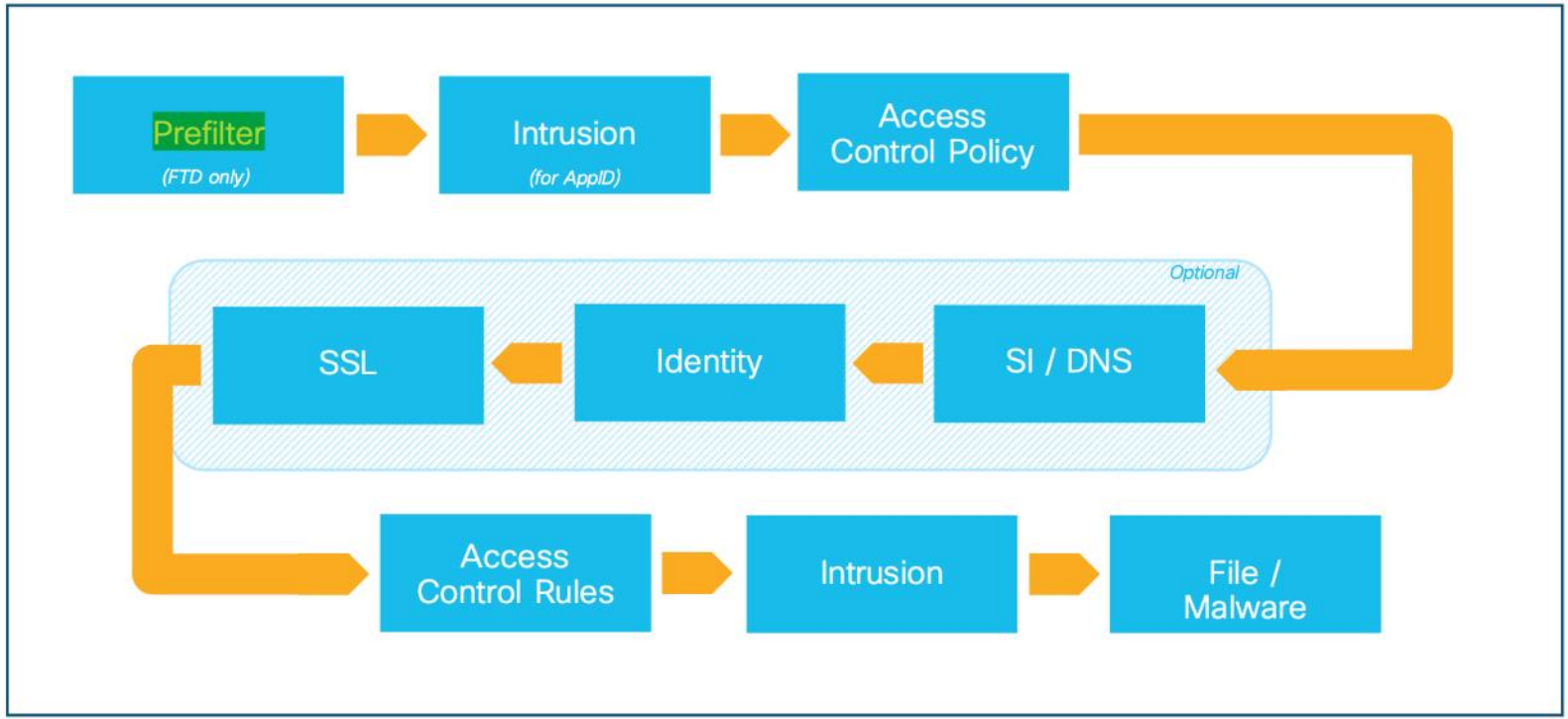


① Analysisを選択
② Hosts>Network Mapを選択

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

6. Prefilterの設定

FTD処理順序概要

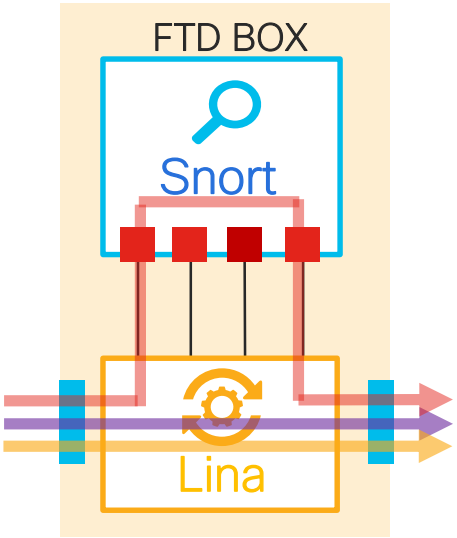


Prefilter概要

- ASAエンジンでL2-L4のみ処理するため、高速な通信制御が可能になる
- トンネル(GRE、IP-in-IP、IPv6-in-IP、Teredo Port 3544)内のパケットをInspectionできる
- 不要な通信をSnortエンジンに渡さずBlockすることで、パフォーマンスを最適化できる
- SnortルールやVDB更新時などに発生するSnort再起動による通信影響を、Fastpathすることで 回避できる (Fastpath: Snort処理を完全にバイパス)

【Prefilterの利用ケース例】
- Snortエンジンを経由しなくても良い信頼された大容量バックアップ通信や暗号化通信をFastpathする
- 死活監視やUDP SyslogなどSnort 再起動時にダウンさせたくない通信をFastpathする
- 明らかに不正なIPアドレスからの通信をSnortエンジンを介さずにBlockする
- 存在しないもしくは許可しないIP アドレス宛の通信をSnortエンジンを介さずにPrefilterでBlockする
- ASA移行ツールから移行されるアクセスコントロールエントリ(ACE)のプレースホルダーとして機能する

Snort リスタートによる影響を回避



- fastpathされたコネクションは、Snort リスタートによる影響を受けない

Default
Flow Preservation、Fail-Open
Prefilter (Fastpath)

Prefilter と Access Control Policy との違い

	Prefilter	Access Control Policy
設定箇所	Policies > Access Control > Prefilter	Policies > Access Control > Access Control
処理エンジン	ASAエンジン	ASAエンジン＋Snortエンジン (設定内容により変化)
Rule Action	Analyze Fastpath Block	Trust, Permit, monitor, Block, Interactive Block, Deep Inspection など
Rule Criteria	Interface、Network、VLAN tag、Port	多数 (URLやアプリケーション情報、 地理情報なども利用可)
ロギング	Fastpathと Blockのみ設定可 Analyzeは不可 (Analyzeは後続処理のロギング設定に依存)	全てのコネクションで対応
処理順序	アクセス制御処理の中で最初に実行	(設定内容により可変)
処理速度	高速	(設定内容により可変)

参考：Prefilter(Tunnel Rule)のフィルタについて

- Prefilter(Tunnel Rule)のフィルタは、トンネル(GRE、IP-in-IP、IPv6-in-IP、Teredo Port 3544)トラフィックの外部IPヘッダに基づいてフィルタリングする

Prefilterは外部IPヘッダを参照

L2 Header	Outer IP Header	GRE Header	Inner IP Header	L7
	src=192.168.75.39 dst=192.168.76.39		src=10.0.0.1 dst=10.0.0.2	

Access Control Policyは内部IPヘッダを参照

L2 Header	Outer IP Header	GRE Header	Inner IP Header	L7
	src=192.168.75.39 dst=192.168.76.39		src=10.0.0.1 dst=10.0.0.2	

参考：PrefilterのActionについて

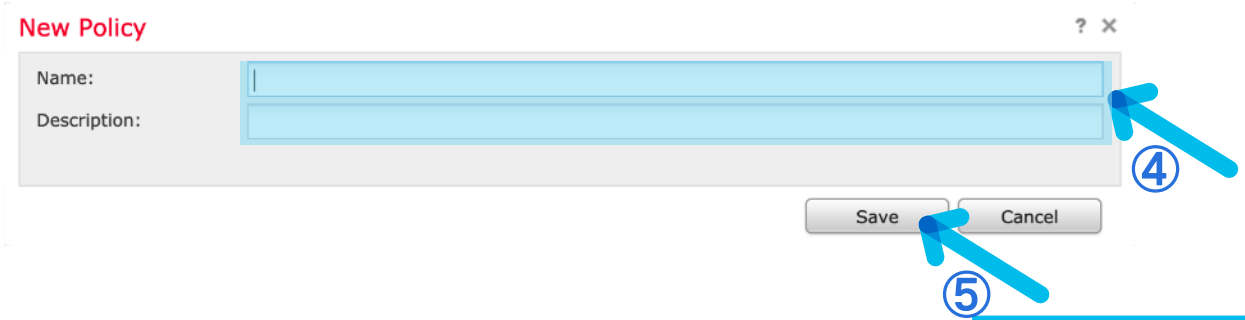
アクション	説明
Analyze (Default)	LINAエンジンの後にSnortエンジンによってチェックされる。オプションでトンネルされたトラフィックにタグを割り当てることができる。Prefilterのロギング設定ができない。
Block	フローはASAエンジンによってブロックされる。トンネルの外部ヘッダーがチェックされる。
Fastpath	フローはASAエンジンによってのみ処理される。Snortエンジンを使用しない。

Prefilter(Prefilter Rule)設定

参考シナリオ：Local Network(192.168.1.0)**を双方向で**Fastpath**する設定**

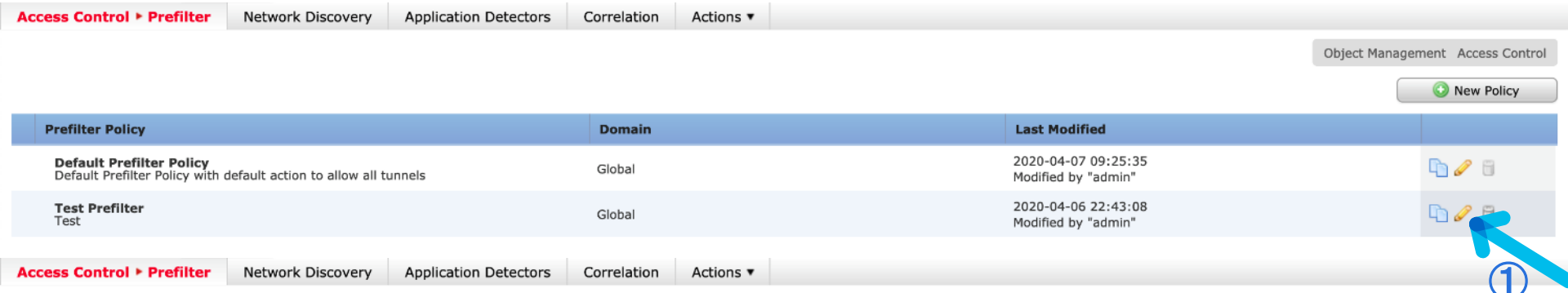
※作成が不要な場合はスキップ

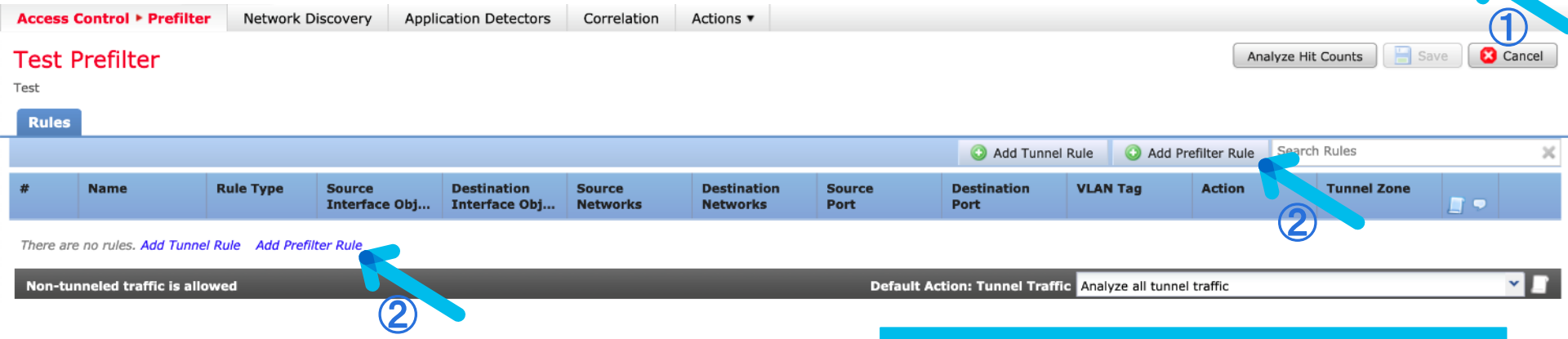
ステップ2-1：Prefilter(Prefilter Rule)の作成



① Policiesを選択
② Prefilterを選択
③ New Policyを選択
④ 任意の名前とDescription(Option)を入力
⑤ “Save”を選択

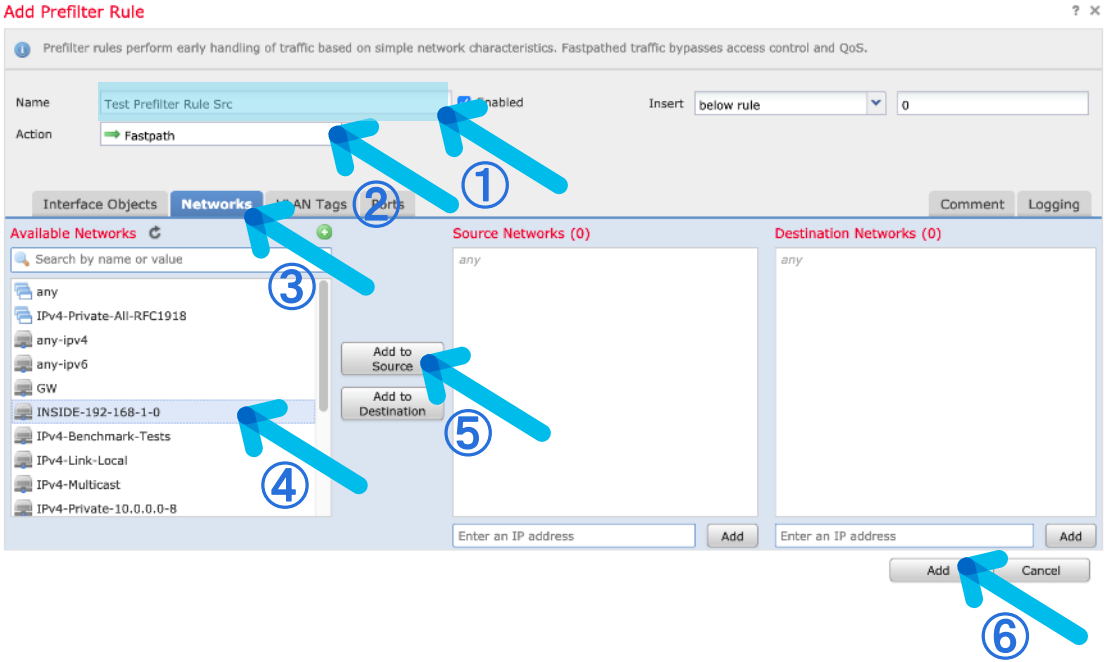
ステップ2-2：Prefilter(Prefilter Rule)の作成





① 作成したPrefilterの鉛筆マークを選択
② Add Prefilter Ruleを選択

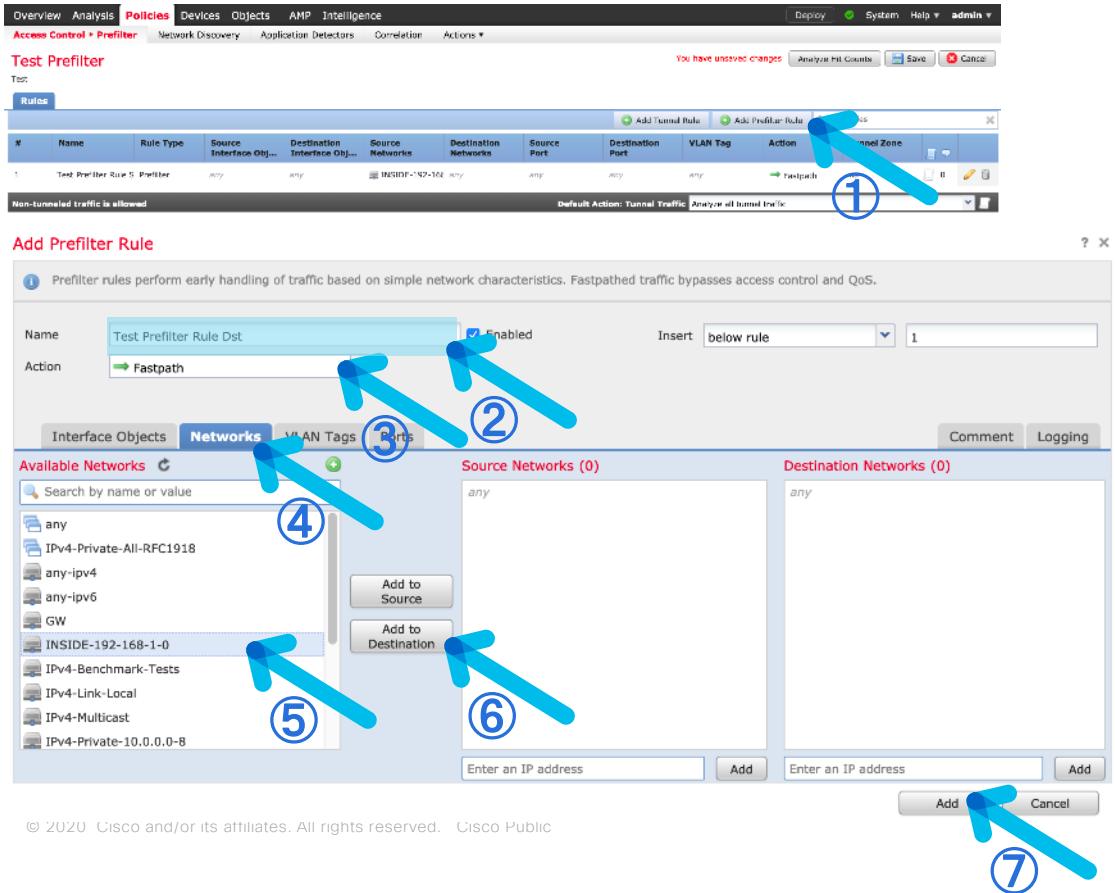
ステップ2-3：Prefilter(Prefilter Rule)の作成



1行目のruleを作成

① 任意の名前を入力
② Fastpathを選択
③ Networksを選択
④ Fastpathを適用するNetworkを選択
⑤ Add to Sourceを選択
⑥ “Add”を選択

ステップ2-4：Prefilter(Prefilter Rule)の作成

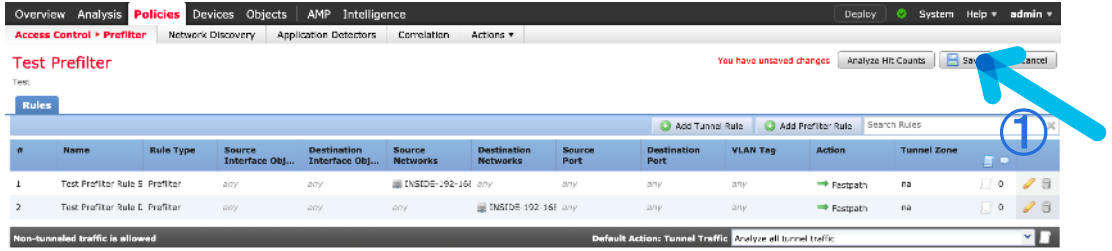


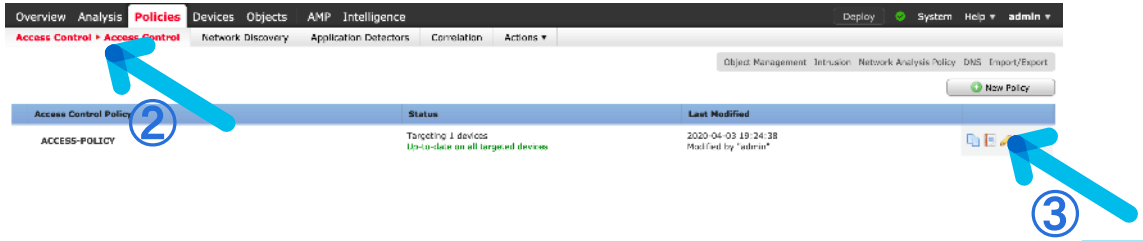
2行目のruleを作成

Logging設定は任意

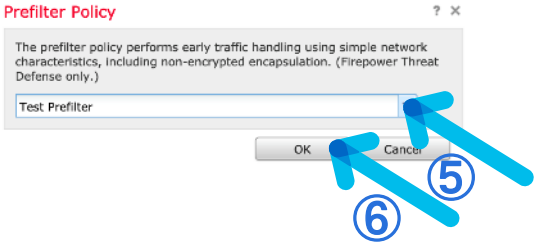
① Add Prefilter Ruleを選択
② 任意の名前を入力
③ Fastpathを選択
④ Networksを選択
⑤ Fastpathを適用するNetworkを選択
⑥ Add to Destinationを選択
⑦ “Add”を選択

ステップ2-5：Prefilter(Prefilter Rule)の作成



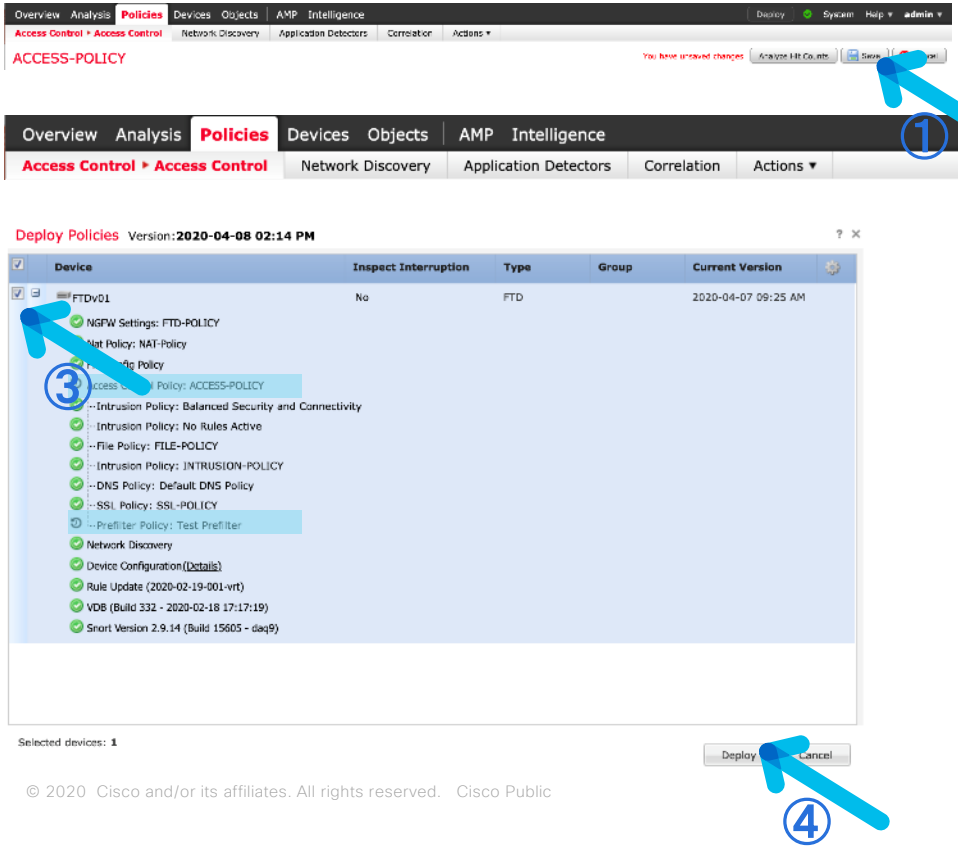


Access Control Policyにこの
Prefilter Policyを紐つける



① ”Save”を選択
② Access Control > Access Controlを選択
③ Prefilterを適用するAccess Control Policyの鉛筆マークを選択
④ Prefilter Policyを選択
⑤ 作成したPrefilterを選択
⑥ “OK”を選択

ステップ2-6：Prefilter(Prefilter Rule)の作成



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

7. Intrusion Policyの設定

Intrusion Policy概要(1/2)

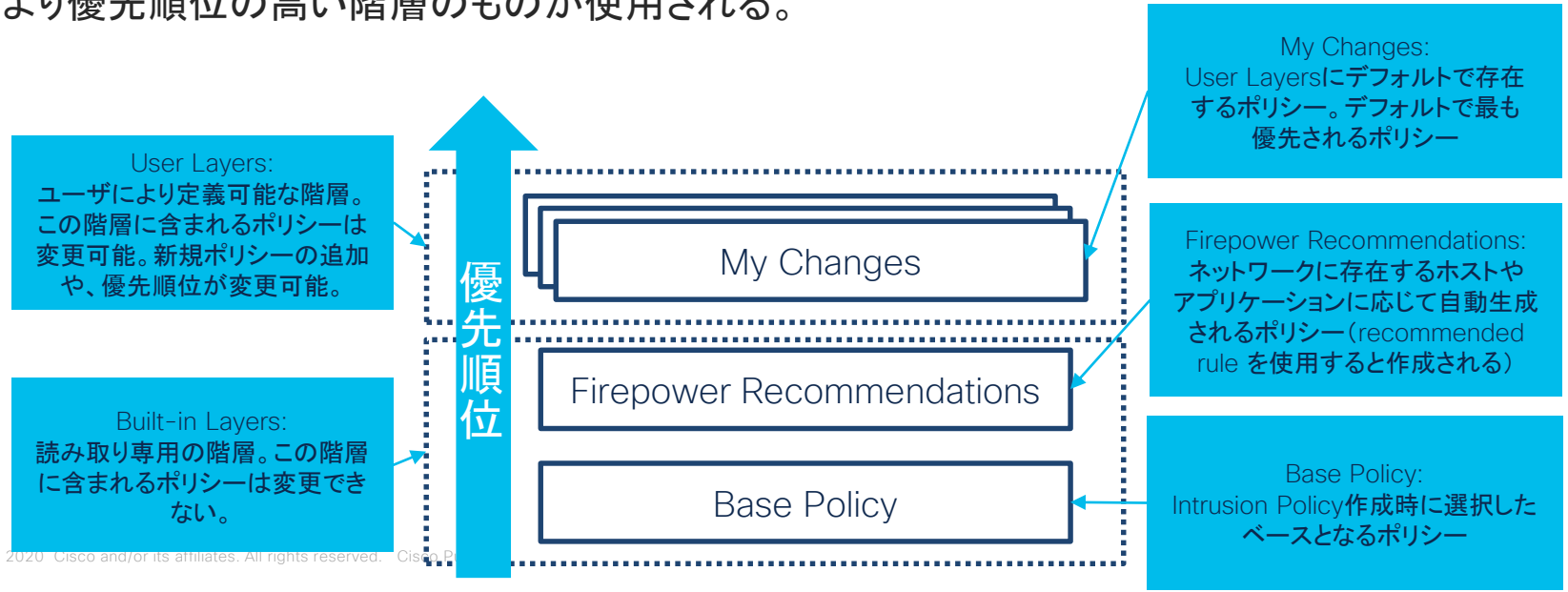
Intrusion Policyにはシグネチャに対するパラメータが含まれ、トラフィックに対するIPSの振る舞いを制御する。

■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。



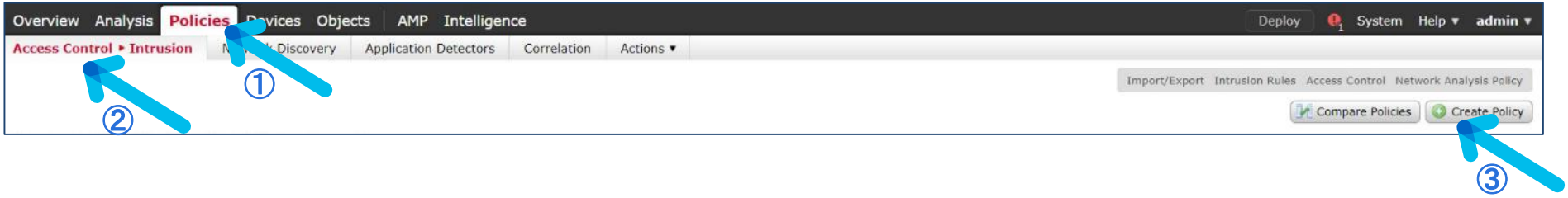
今回設定するIntrusion Policyについて

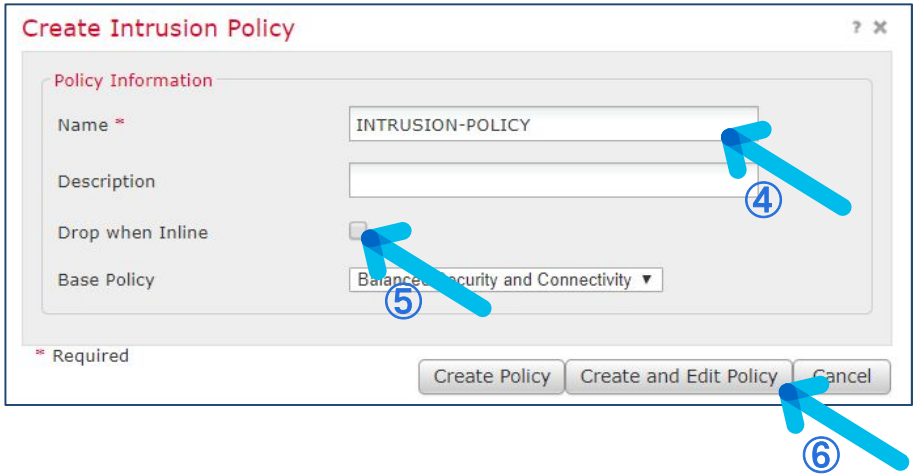
- 評価を目的としているため、トラフィックに影響を与えない様シグネチャヒット時にパケットを破棄しないポリシーを作成する。実環境ではパケットを実際に破棄することも検討すべきである。
- 有意義な評価を行うために、例として一般的な環境でヒットしやすい一部のシグネチャを手動で有効にする。ステップ2: POV用にシグネチャの手動設定①~⑤がこれにあたる。実環境ではこれらを手動で有効にすることは必須ではない。
- IPS機能が正常に動作していることを確認するために、Pingでヒットするシグネチャを手動で有効にする。ステップ2: POV用にシグネチャの手動設定⑥~⑦がこれにあたる。実環境ではこれらを手動で有効にすることは必須ではない。
- Eicar (Malwareテスト通信) についてはIPSではなく後述のFileポリシーでの検知を行うために該当するシグニチャを手動で無効にする。ステップ2: POV用にシグネチャの手動設定⑧~⑨がこれにあたる。実環境では任意。

設定の流れ

- ステップ1：Intrusion Policy の作成
- ステップ2：POV用にシグネチャの手動設定

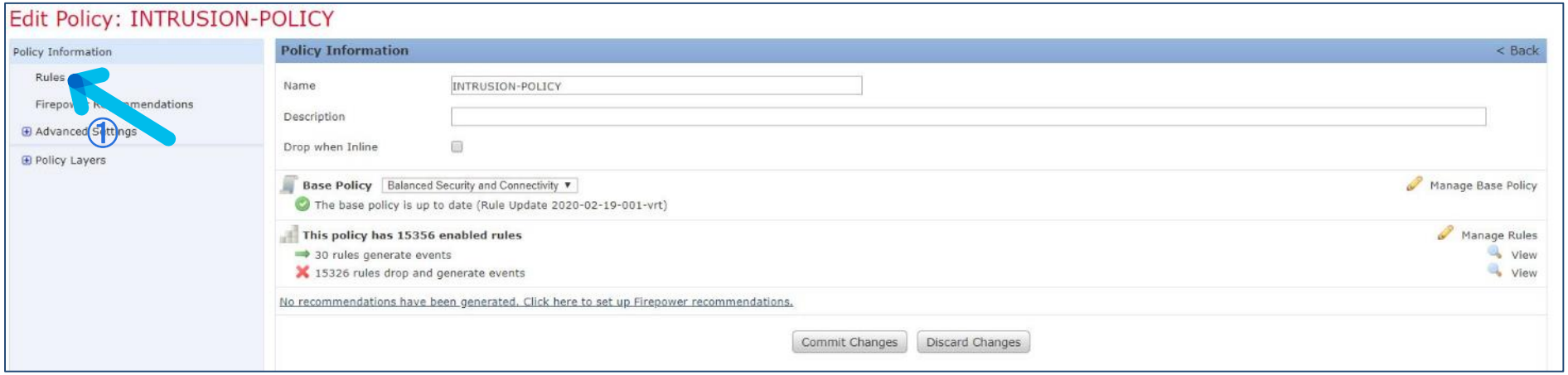
ステップ1 Intrusion Policyの作成





① Policiesを選択
② Access Control下のIntrusionを選択
③ “Create Policy”をクリック
④ Nameを入力。本資料では”INTRUSION-POLICY”とする
⑤ “Drop when Inline”のチェックを外す。(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)
⑥ ”Create and Edit Policy”をクリック

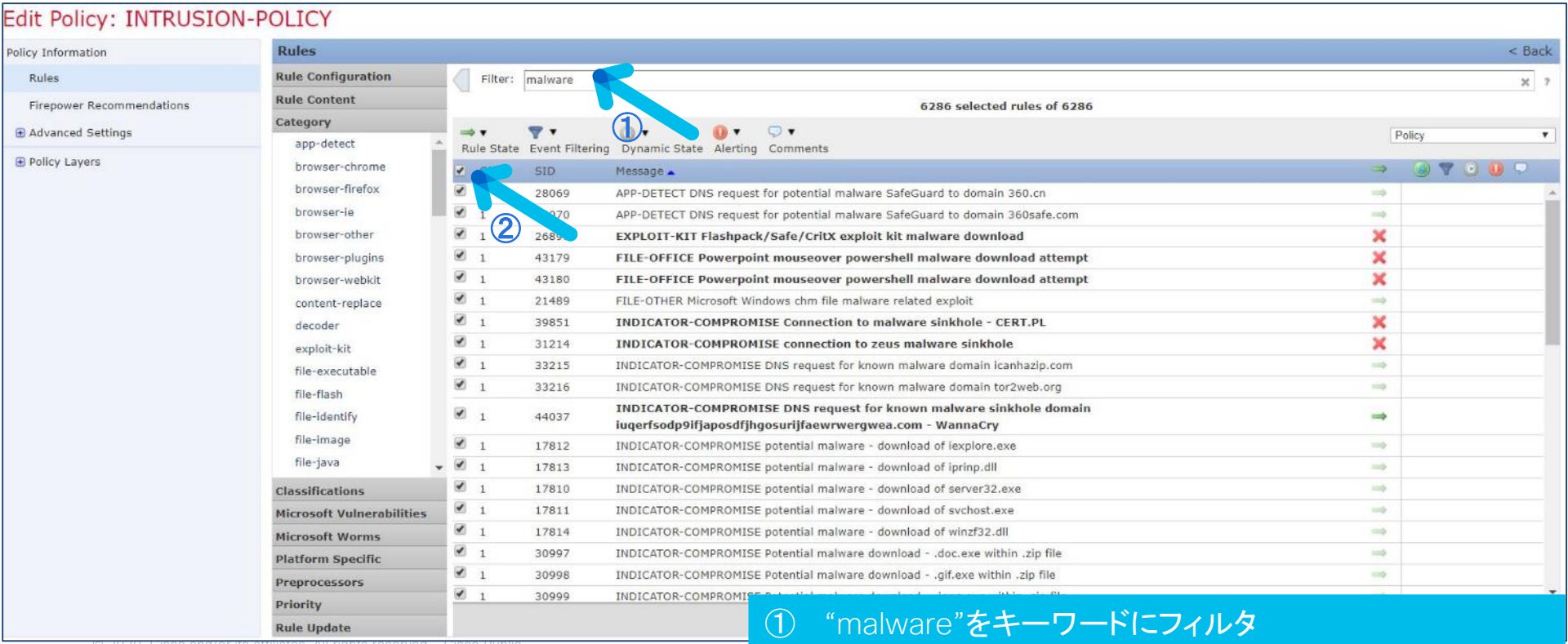
ステップ2：POV用にシグネチャの手動設定①



① Rulesをクリック

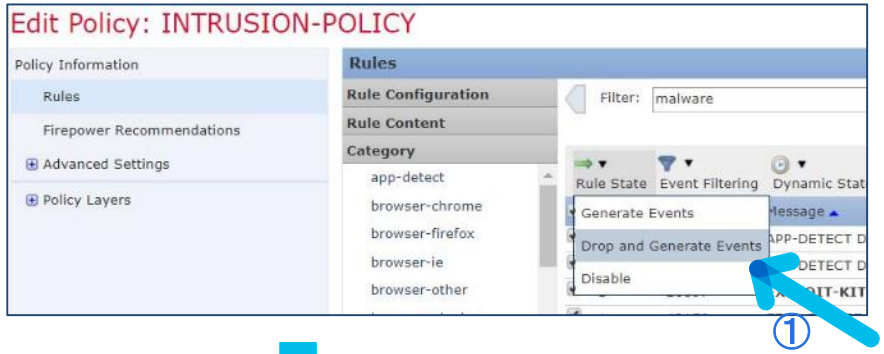
- Intrusion Rule一覧画面から鉛筆アイコンをクリックしても、同様にEdit Policy画面が表示される

ステップ2：POV用にシグネチャの手動設定②



① “malware”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

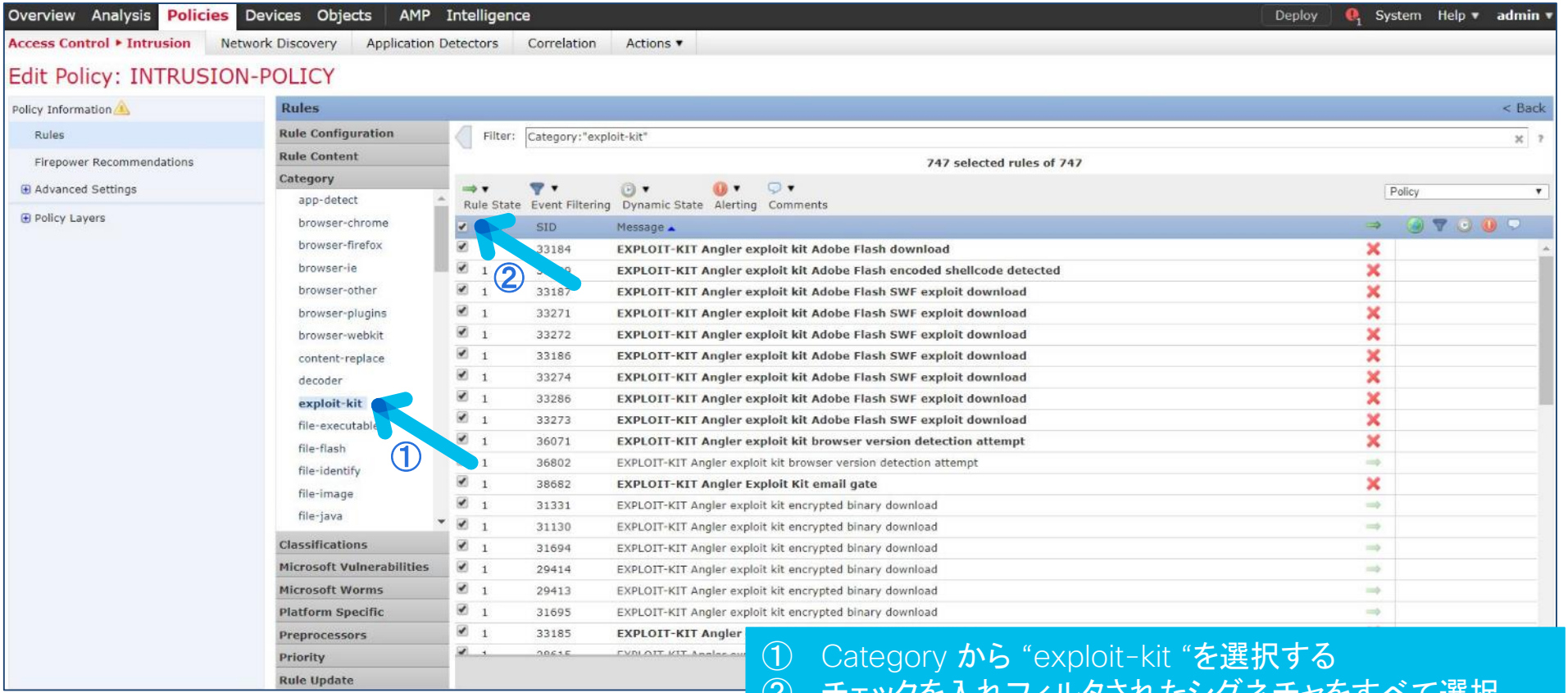
ステップ2：POV用にシグネチャの手動設定③



① Rule State ドロップダウンメニューを開き、Drop and Generate Events を選択
② 正常に変更が完了したらプロンプトが表示されるので”OK”をクリック

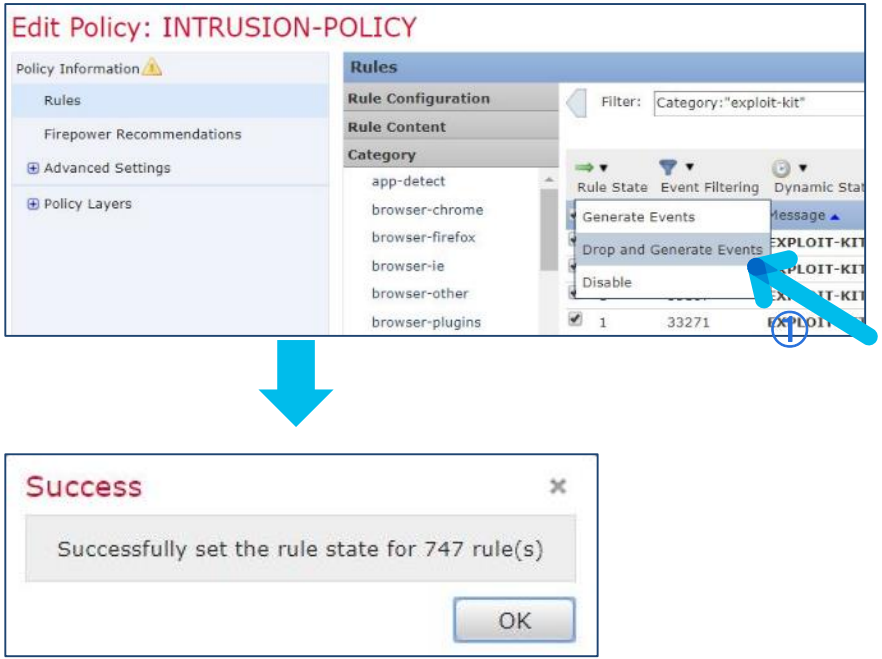
- 同様の操作を、”Blacklist”、”PUA” というキーワードで実施する

ステップ2：POV用にシグネチャの手動設定④



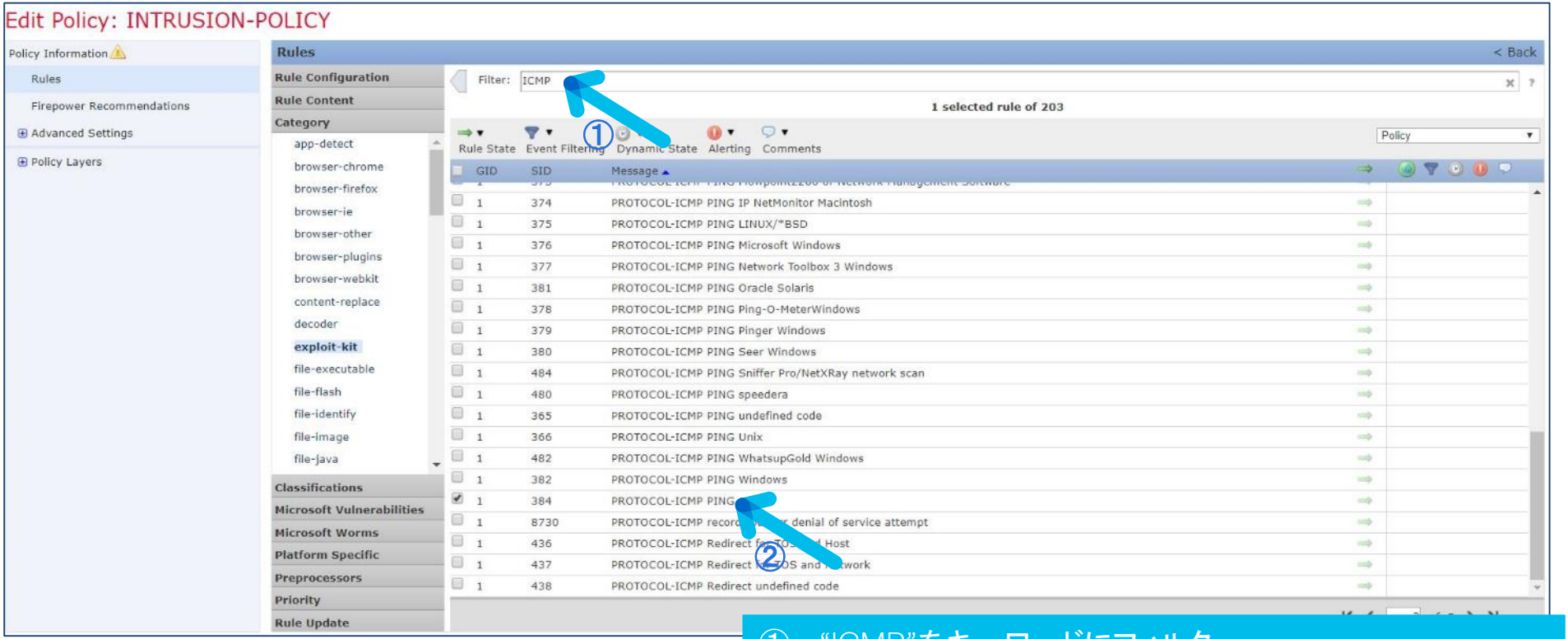
① Category から “exploit-kit “を選択する
② チェックを入れフィルタされたシグネチャをすべて選択

ステップ2：POV用にシグネチャの手動設定⑤



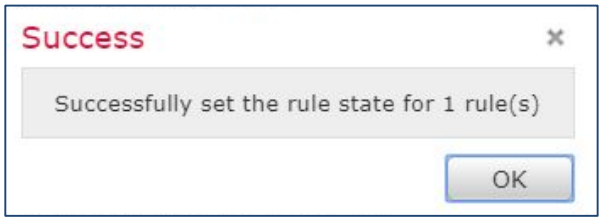
① Rule State ドロップダウンメニューを開き、Drop and Generate Events を選択
② 正常に変更が完了したらプロンプトが表示されるので”OK”をクリック

ステップ2：POV用にシグネチャの手動設定⑥



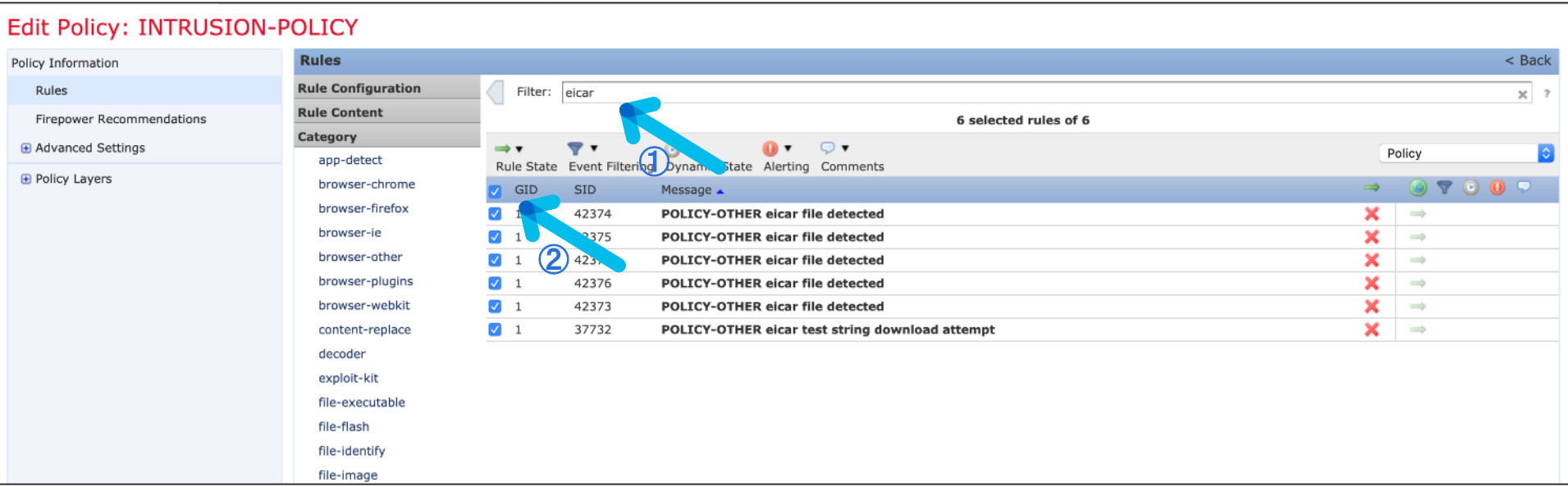
① “ICMP”をキーワードにフィルタ
② GID1 SID384の”PROTOCOL-ICMP PING”をチェック

ステップ2：POV用にシグネチャの手動設定⑦



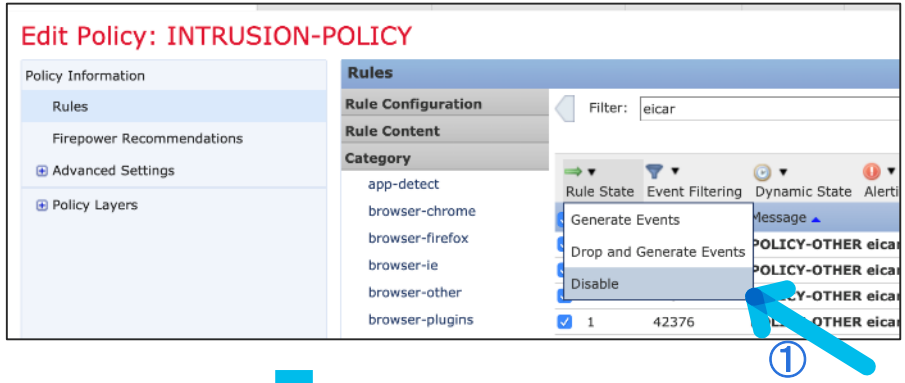
① Rule State ドロップダウンメニューを開き、Drop and Generate Events を選択
② 正常に変更が完了したらプロンプトが表示されるので”OK”をクリック

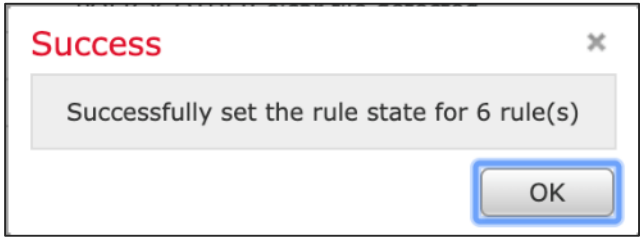
ステップ2：POV用にシグネチャの手動設定⑧



① “eicar”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

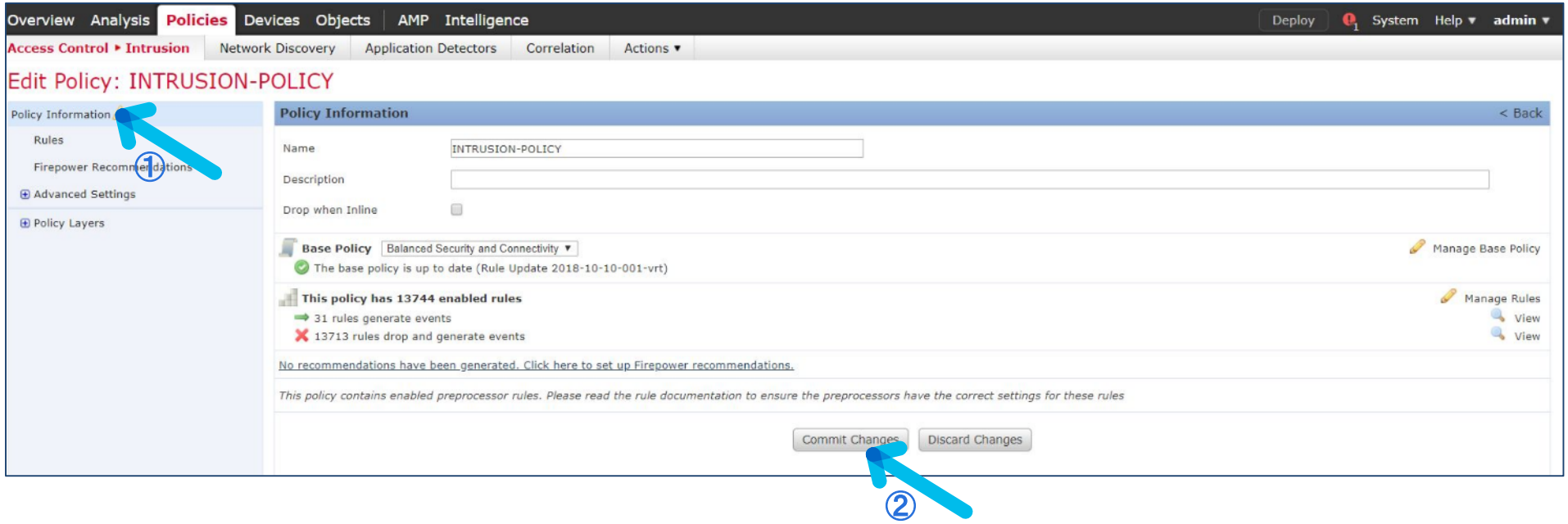
ステップ2：POV用にシグネチャの手動設定⑨





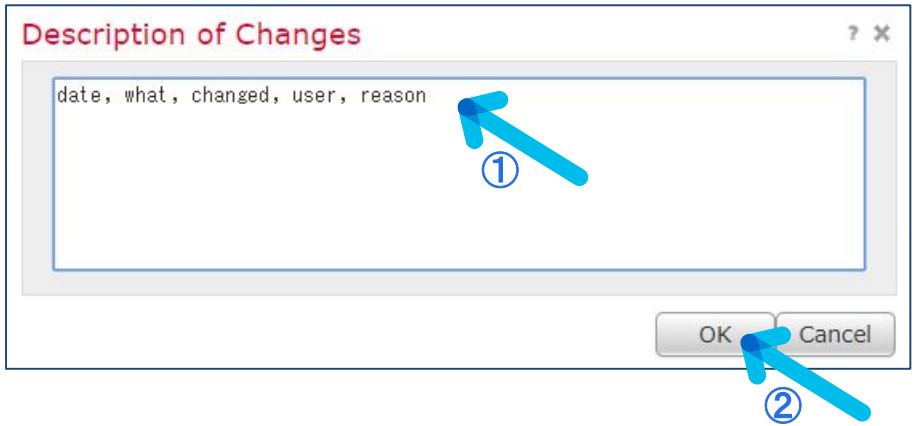
① Rule State ドロップダウンメニューを開き、Disable を選択
② 正常に変更が完了したらプロンプトが表示されるので”OK”をクリック

ステップ2：POV用にシグネチャの手動設定　設定保存①



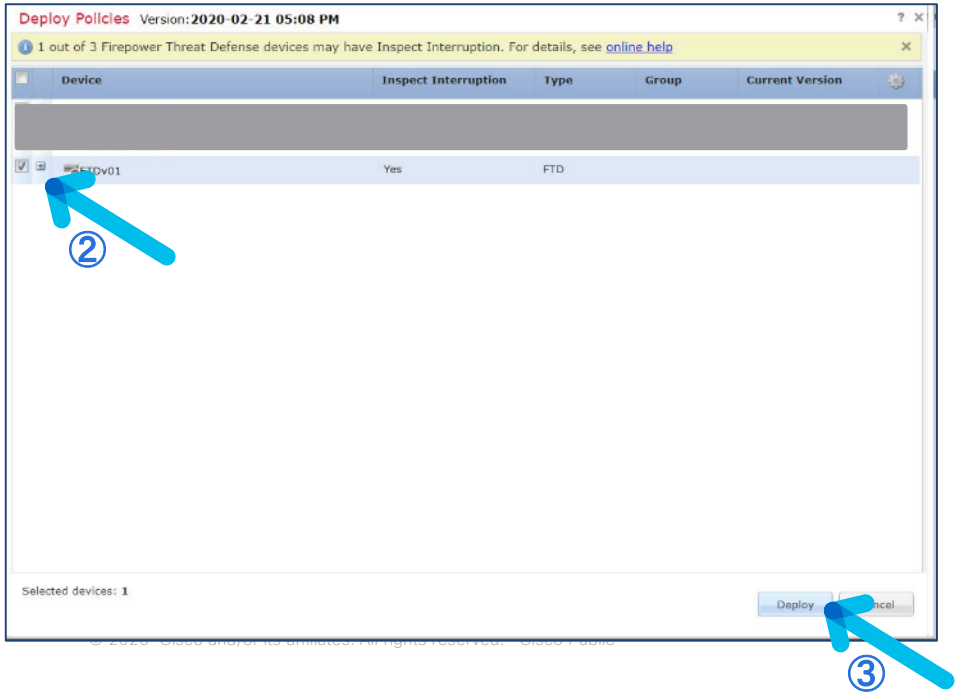
① Policy Informationをクリック
② Commit Changesをクリック

ステップ2：POV用にシグネチャの手動設定　設定保存②



① コメントを記入(任意)
② “OK”をクリック

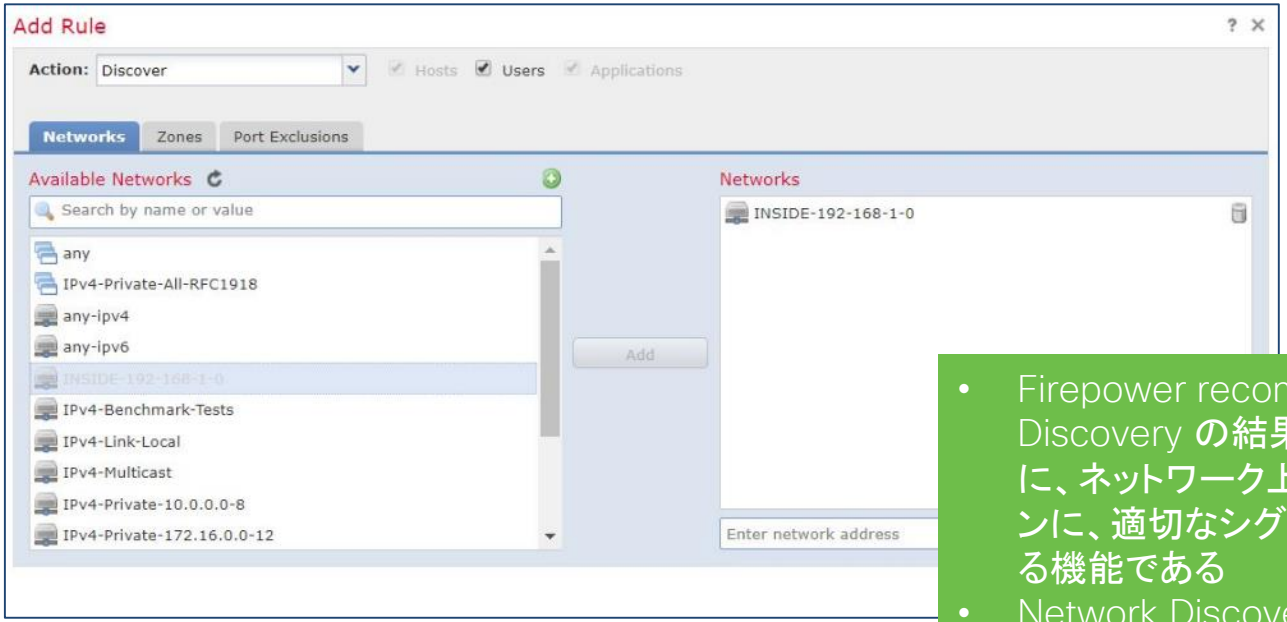
ステップ2：POV用にシグネチャの手動設定　Deploy



① Deployをクリック
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をクリック

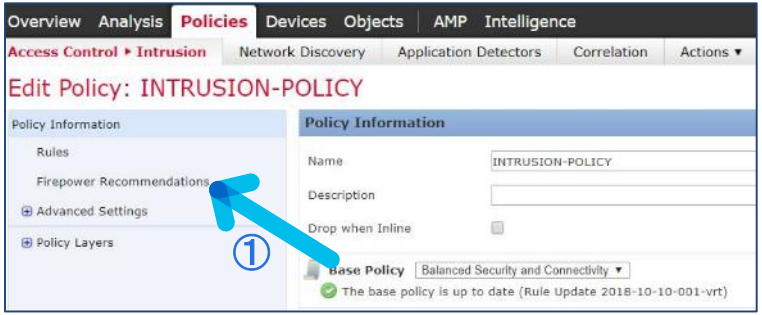
- Deployによってインスペクション処理に影響の出る機器がある場合、”Firepower Threat Defense devices may have Inspect Interruption. For details, see online help”と表示される
- Intrusion PolicyはAccess Control Policyへ割り当てが必要。9章[ステップ 2: Access Rule の設定②]を参照

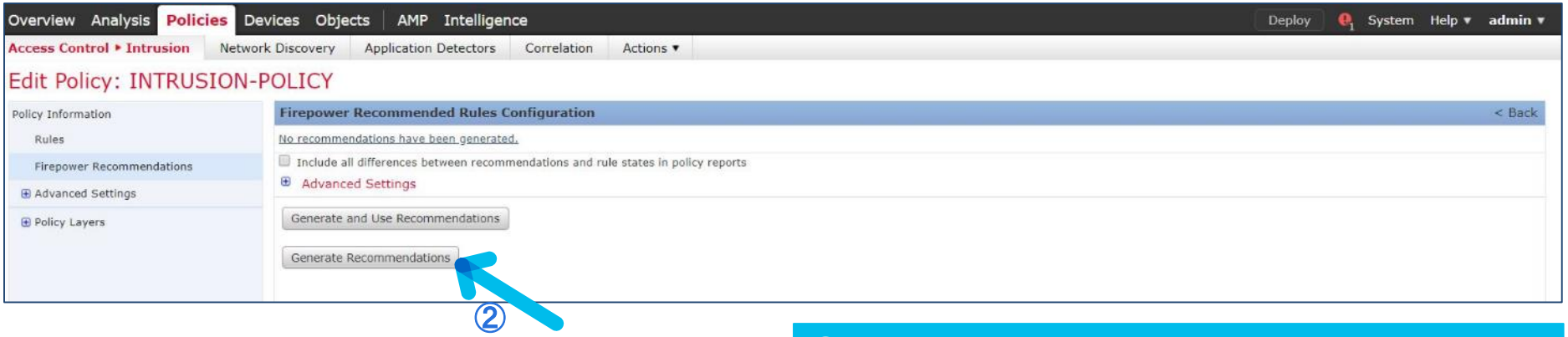
【参考情報】
Firepower recommendation によるルールの最適化



- 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

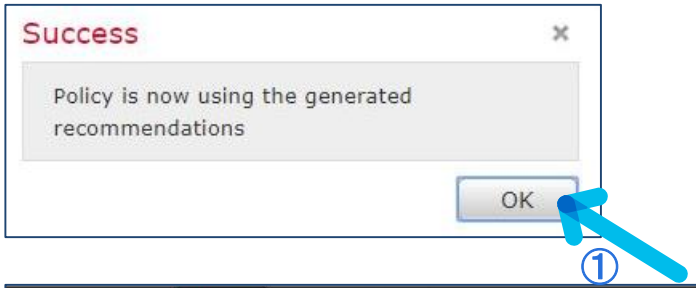
【参考情報】
Firepower recommendation によるルールの最適化





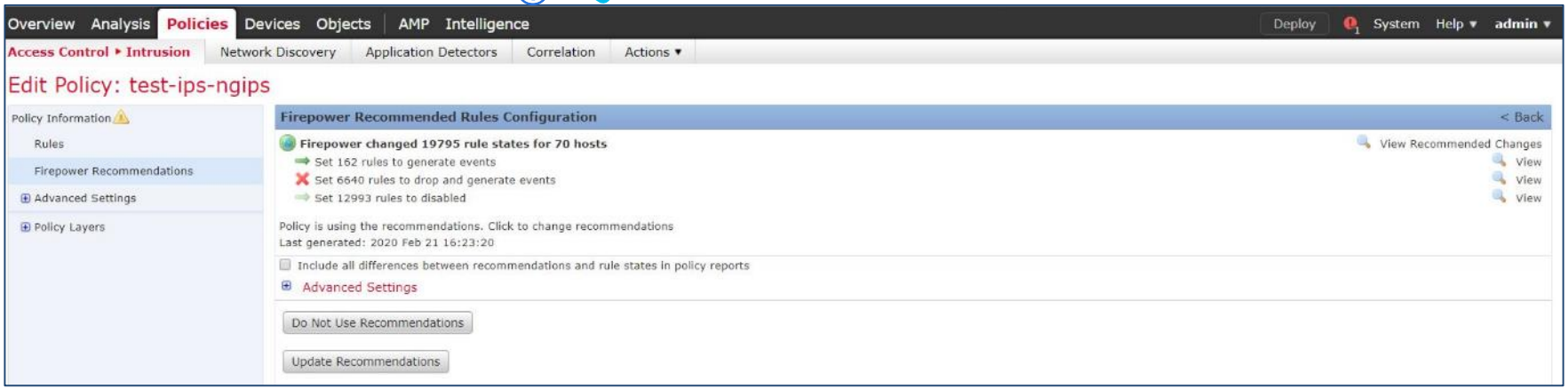
① “Firepower Recommendations”をクリック
② “Generate and Use Recommendations”をクリック

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



① “OK”をクリック

- Firepower recommendationの生成と適用と分割することも可能
- その場合”Generate Recommendations”をクリックした後に、”Use Recommendations”をクリック



8. Malware & File Policyの設定

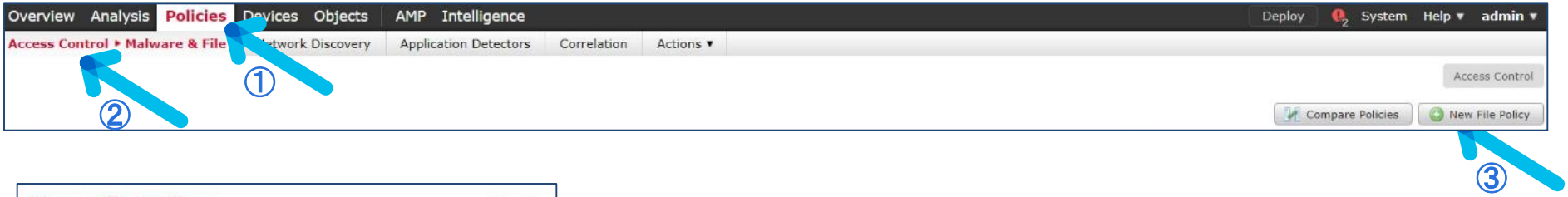
File Policyの概要

- 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

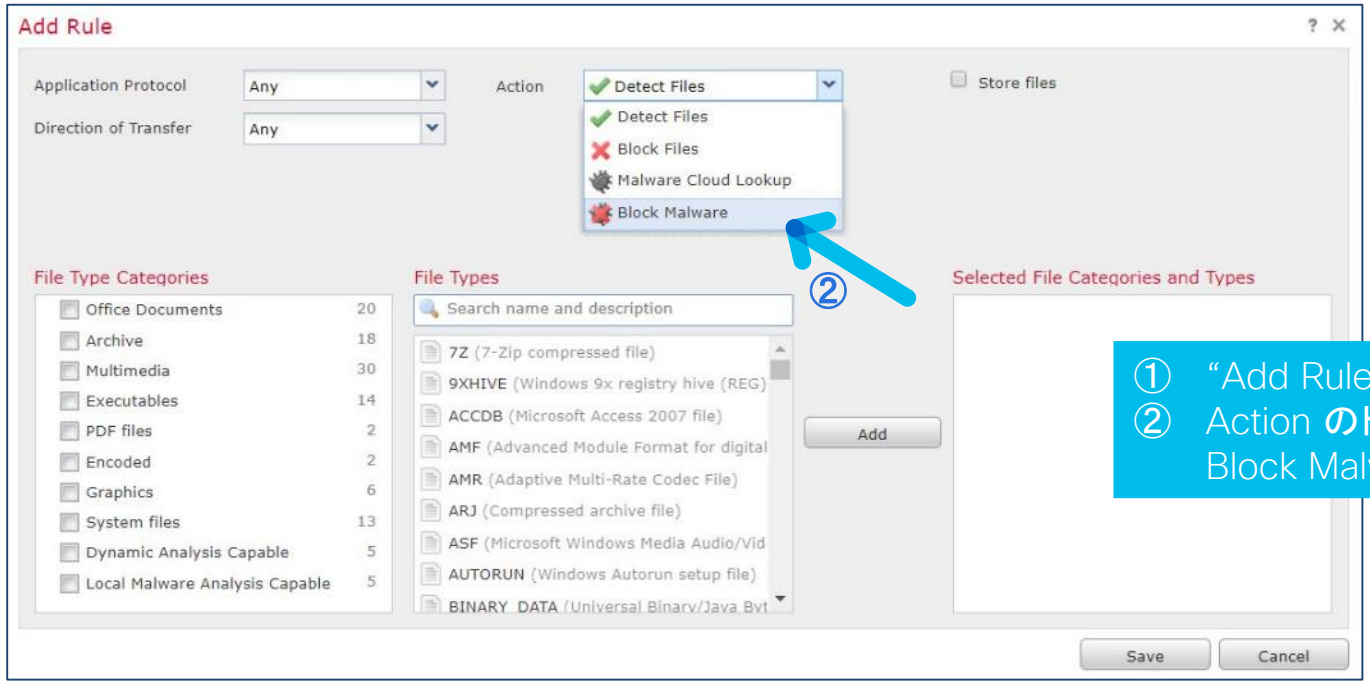
ステップ1: File Policyの作成



① Policiesを選択
② Access Control下のMalware & Fileを選択
③ “New File Policy”をクリック
④ Nameを入力。本資料では” FILE-POLICY”とする
⑤ “Save”をクリック

ステップ2: File Rule(一つ目)の作成①

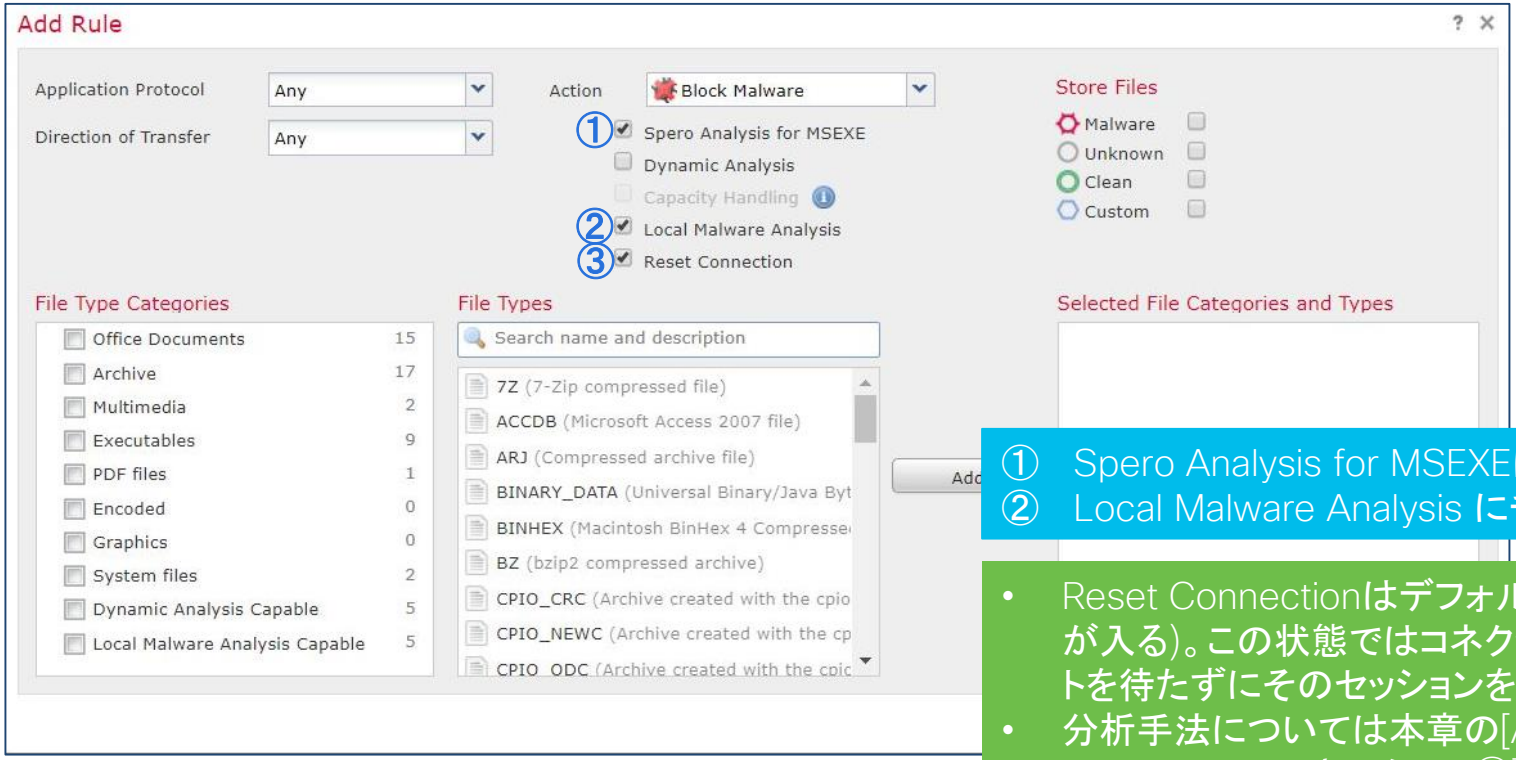
①



②

① “Add Rule”をクリック
② Action のドロップダウンリストを開き、Block Malware を選択する

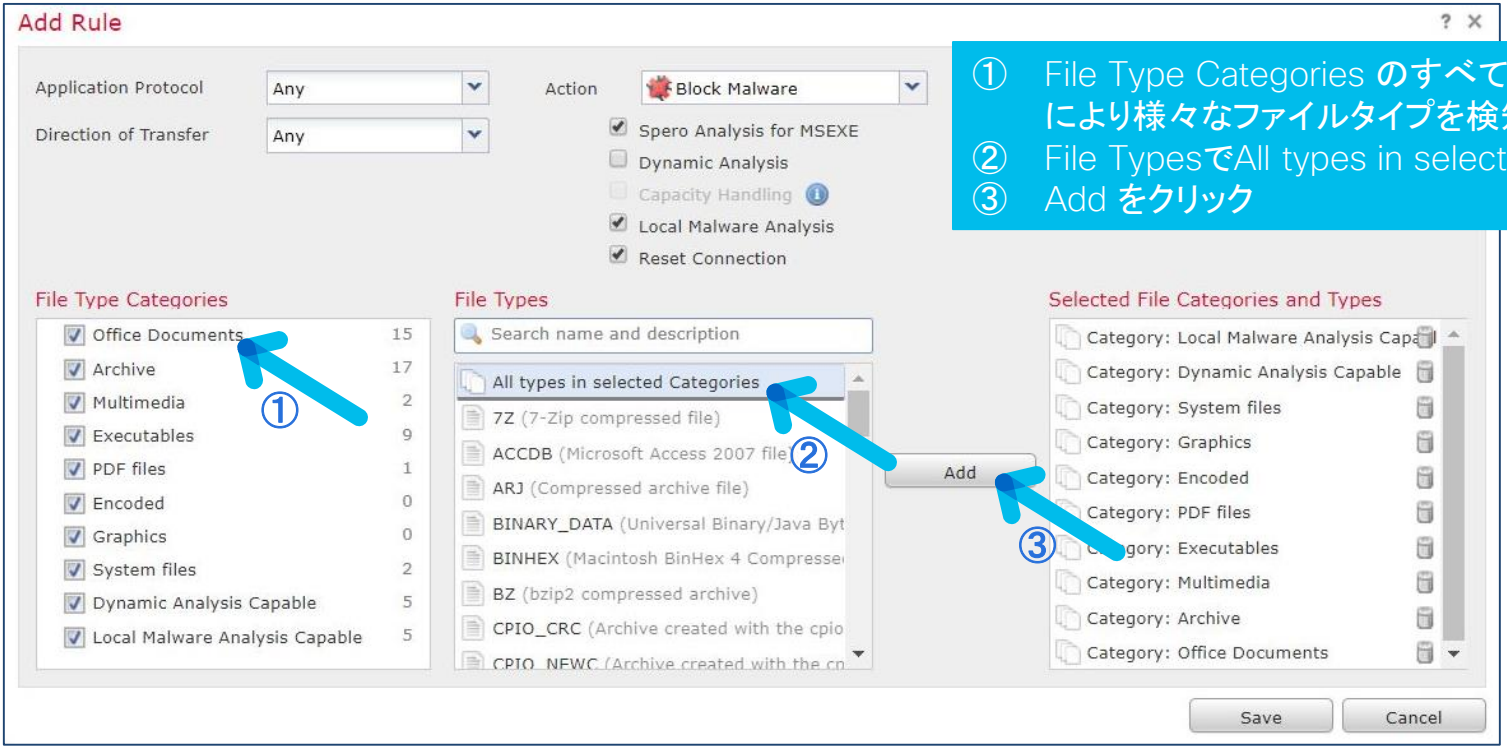
ステップ2: File Rule(一つ目)の作成②



① Spero Analysis for MSEXEにチェックを入れる
② Local Malware Analysis にチェックを入れる

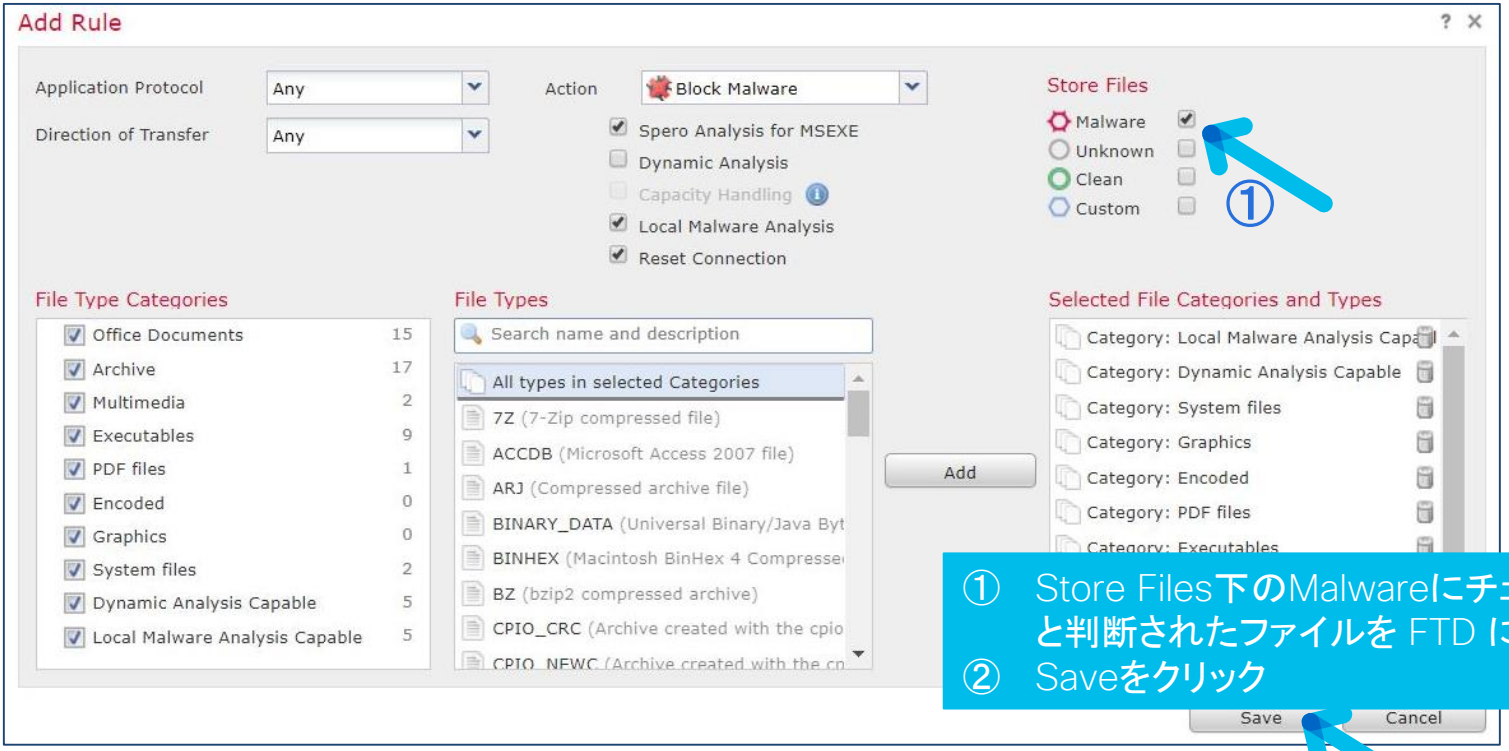
- Reset Connectionはデフォルトで有効(チェックが入る)。この状態ではコネクションのタイムアウトを待たずにそのセッションを終了する
- 分析手法については本章の[AMP for Firepower アーキテクチャ②]を参照

ステップ2: File Rule(一つ目)の作成③



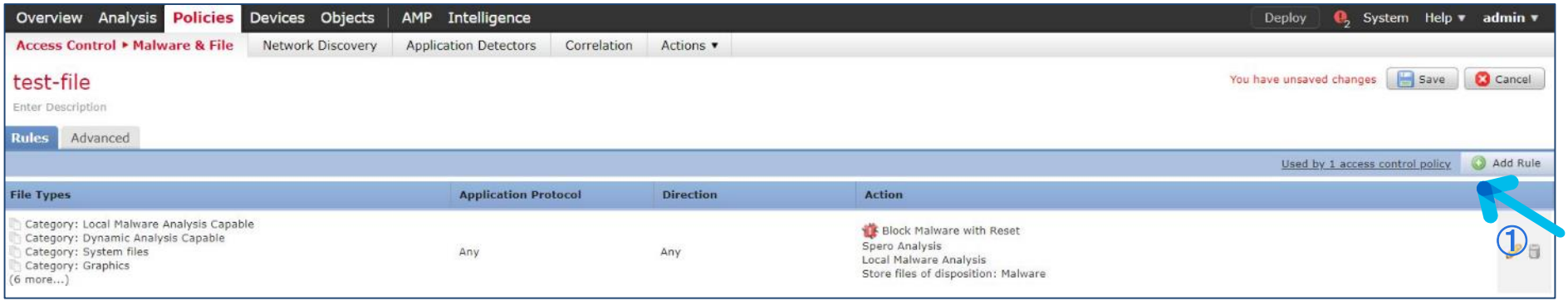
① File Type Categories のすべてにチェックを入れる。これにより様々なファイルタイプを検知できる
② File TypesでAll types in selected Categoriesを選択
③ Add をクリック

ステップ2: File Rule(一つ目)の作成④



① Store Files下のMalwareにチェックを入れる (Malwareと判断されたファイルを FTD に一時保管したい場合)
② Saveをクリック

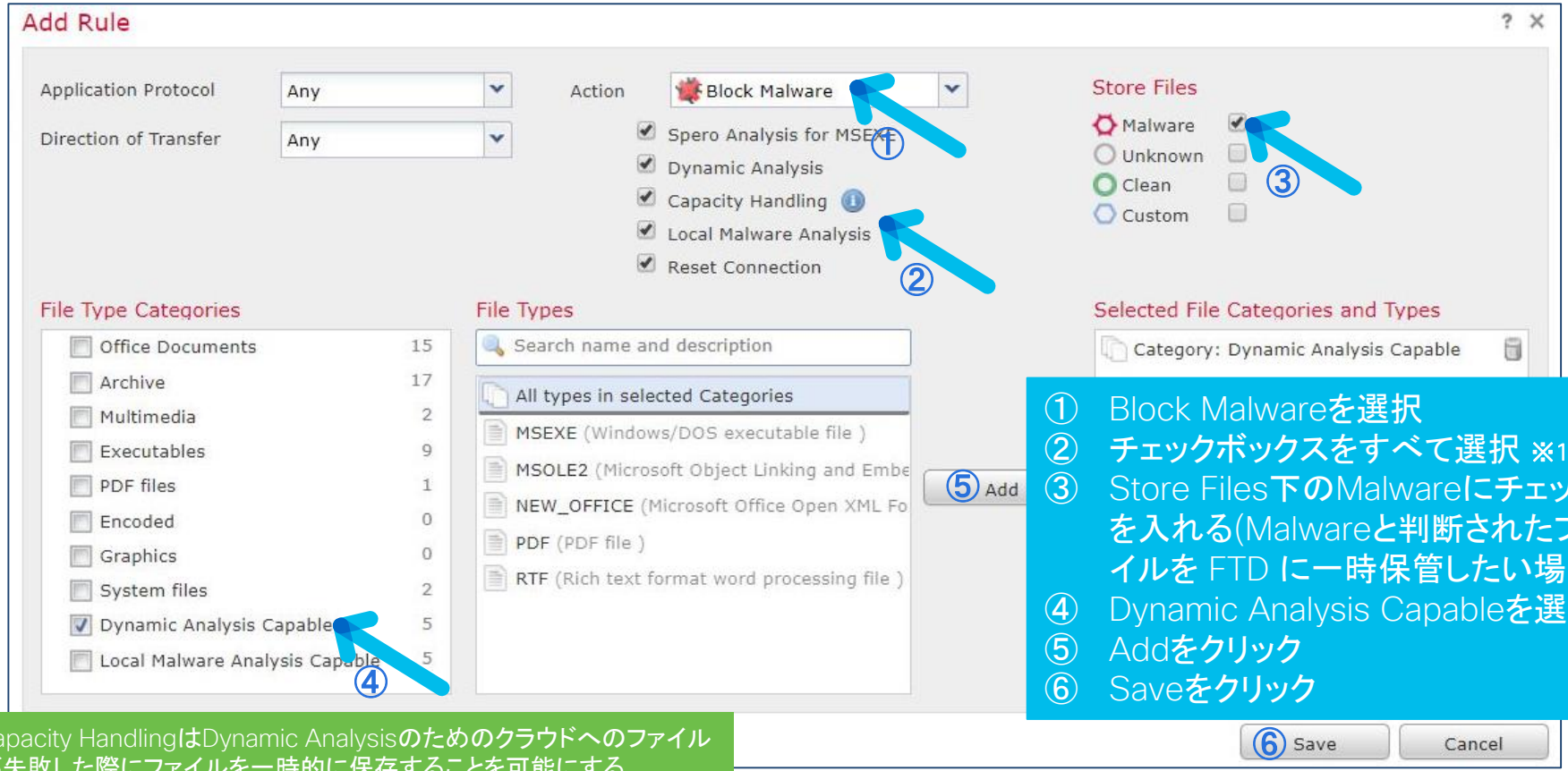
ステップ3: File Rule(二つ目)の作成①



① Add Ruleをクリック

この例では、Dynamic Analysisが可能なファイルはThreat Gridに送るという
上書きルールとして二つ目のルールを作る

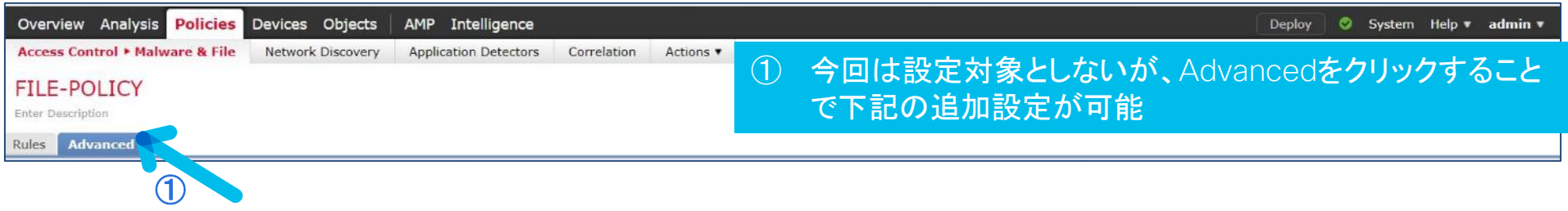
ステップ3: File Rule(二つ目)の作成②

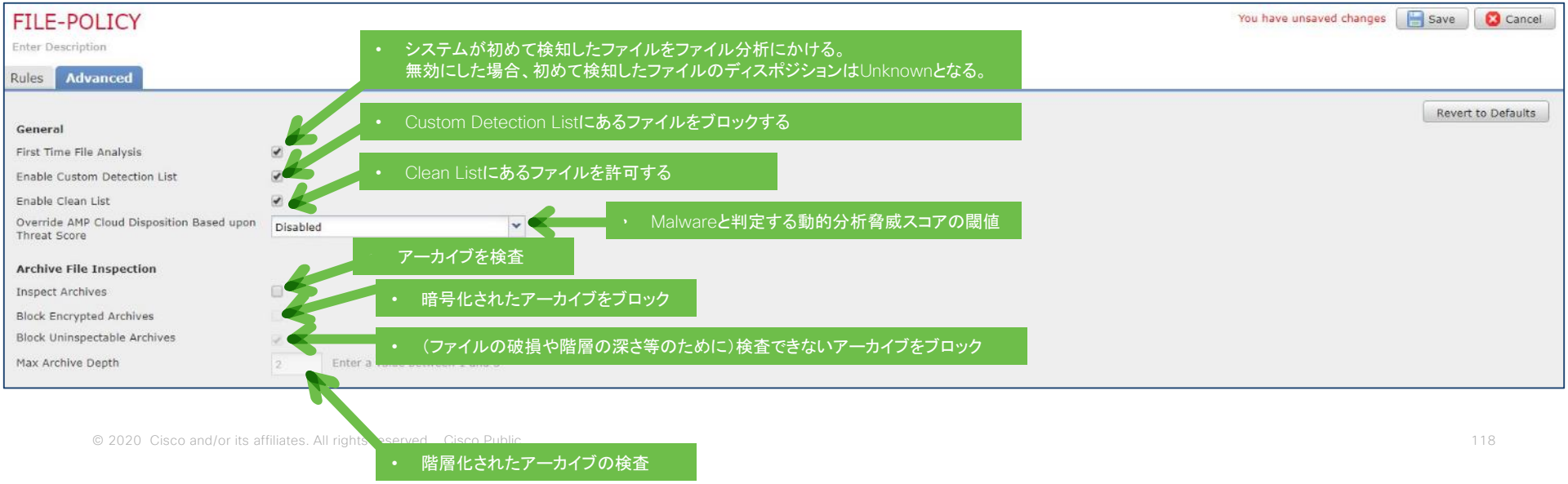


① Block Malwareを選択
② チェックボックスをすべて選択 ※1
③ Store Files下のMalwareにチェックを入れる(Malwareと判断されたファイルを FTD に一時保管したい場合)
④ Dynamic Analysis Capableを選択
⑤ Addをクリック
⑥ Saveをクリック

※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

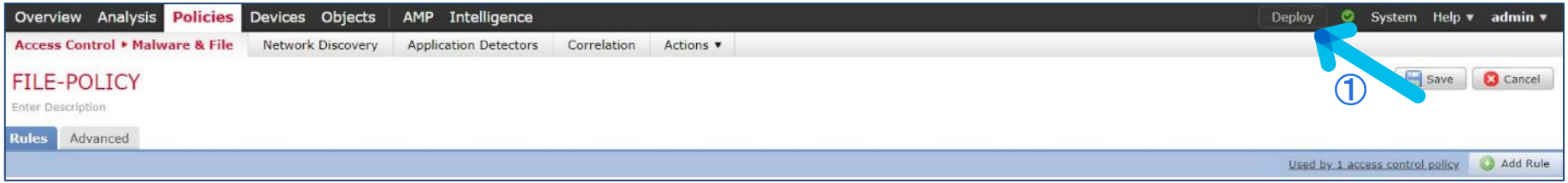


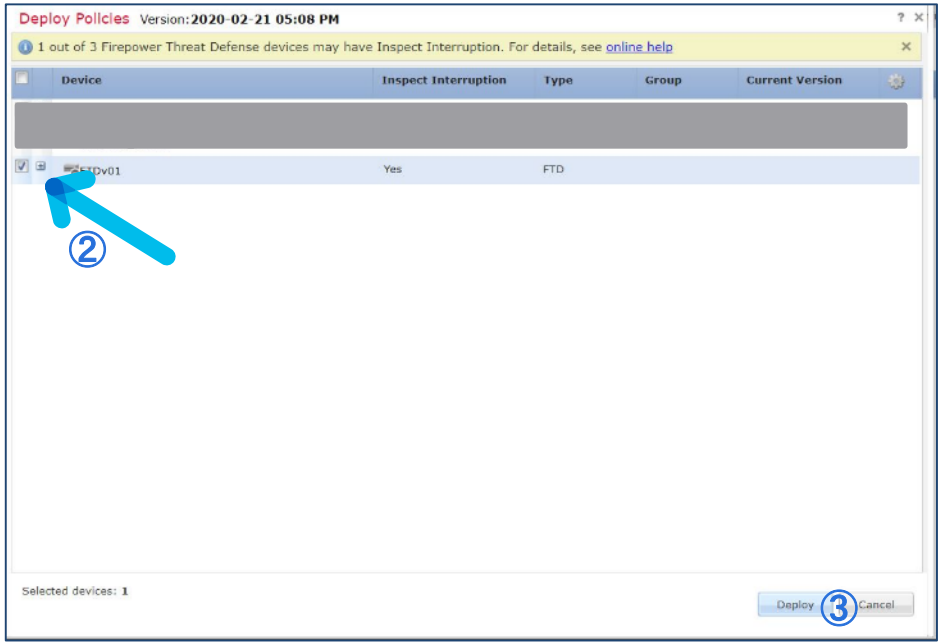


ステップ4: Advancedタブの確認とFile Policy保存②

① Saveをクリック

ステップ5：Deploy

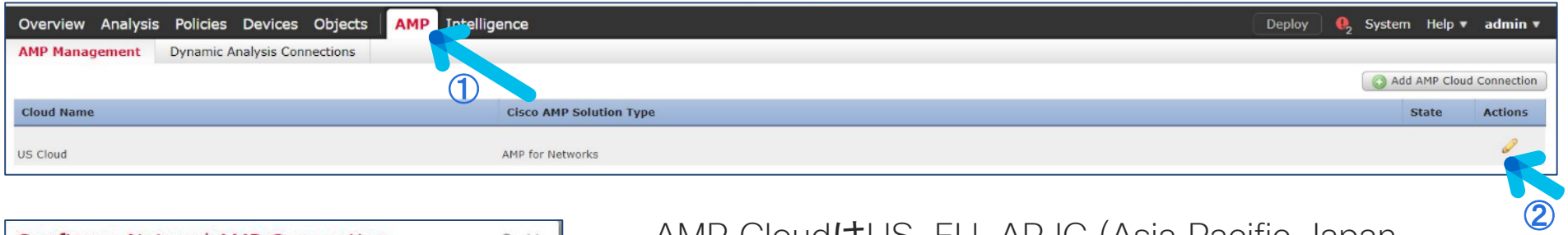


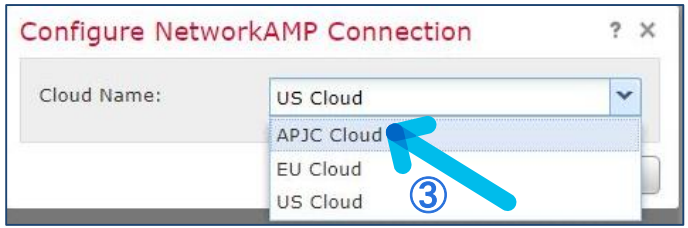


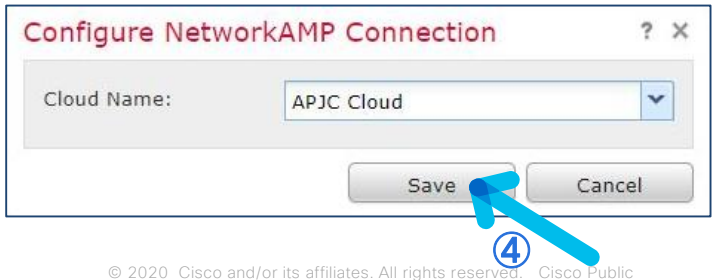
① Deployをクリック
② 変更された設定を確認の上、Deploy対象機器にチェックを入れる
③ Deployをクリック

- Deployによってインスペクション処理に影響の出る機器がある場合、”Firepower Threat Defense devices may have Inspect Interruption. For details, see online help”と表示される
- File PolicyはAccess Control Policyへ割り当てが必要。9章[ステップ 2: Access Rule の設定②]を参照

ステップ6: AMP Cloudの設定







AMP CloudはUS, EU, APJC (Asia Pacific Japan China の略)に設置されており、FMCからいちばん近いCloudを選択することが望ましい。日本に設置したFMCであればAPJC選択を推奨

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
④ Saveをクリック

ステップ7: AMP Threat Gridの設定（確認）

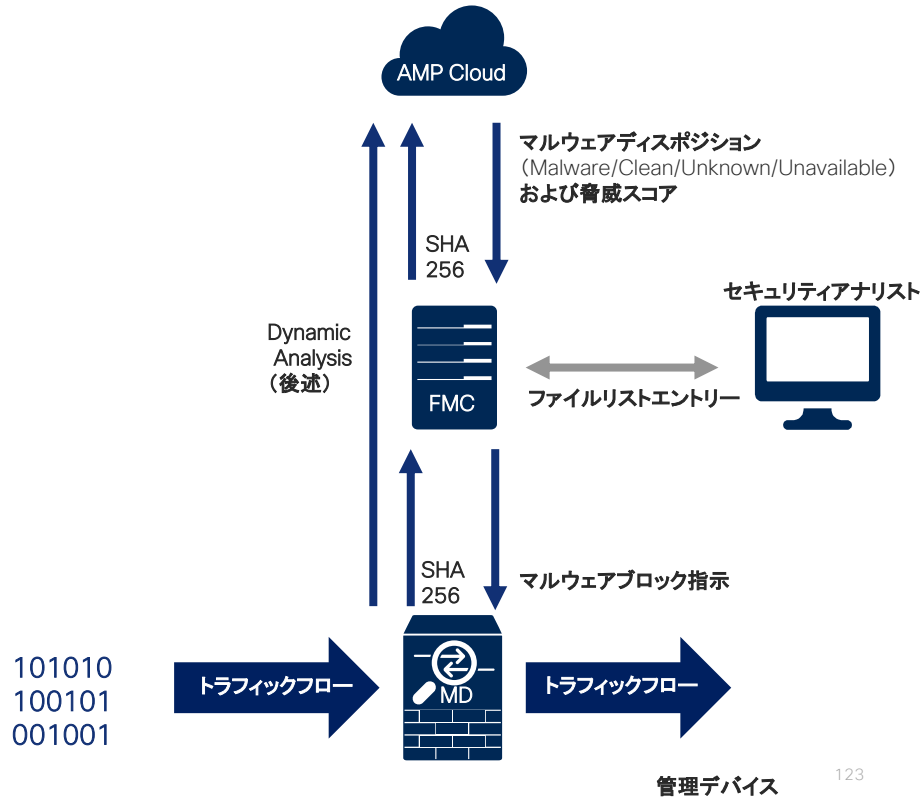
① Dynamic Analysis Connectionsをクリックし、AMP Threat Grid設定を確認

※現時点でThread Gridクラウド環境は、APJCにはない。

AMP for Firepower アーキテクチャ①

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。

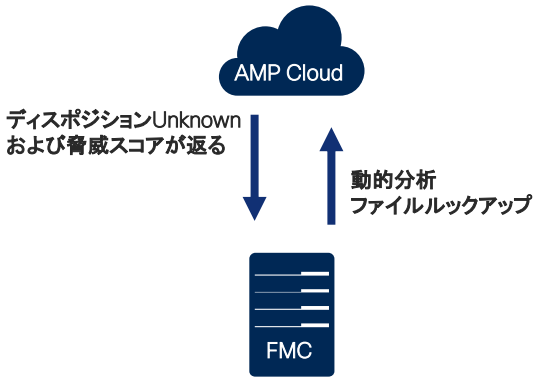
1. ファイル・アーカイブを展開、ファイルハッシュ(SHA-256)は管理デバイス側で計算される
2. 管理デバイスがローカルのキャッシュを参照し、ディスポジションを確認する
3. キャッシュにマルウェアディスポジションが存在しない場合、そのハッシュ値がFMCに送られ、今度はFMCのキャッシュが確認される
4. FMCのキャッシュにもディスポジションがない場合そのハッシュ値をAMP Cloudでルックアップする
5. AMP Cloudからディスポジションが返り、FMC、管理デバイスのキャッシュにディスポジションが登録される
6. ディスポジションがUnknownだった場合、オプションで更なる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



AMP for Firepower アーキテクチャ②

- 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）



分析の順序

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

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

9. Access Control Policyの設定

作成する Access Control Policy について

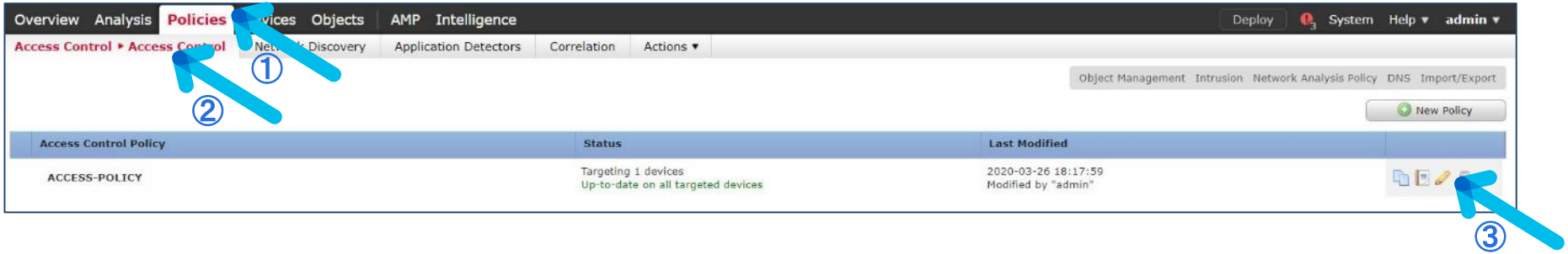
- Security Intelligence によって配信されるネットワークおよび URL の Blacklist はブロックする
- Access Control Policy では、第7~8章で作成した Intrusion Policy と File Policy を使用してセキュリティチェックを行う
- 通信の始まりと終わりのログを取得する
- URLフィルタ機能を使い、Web トラフィックは URL カテゴリーを記録する

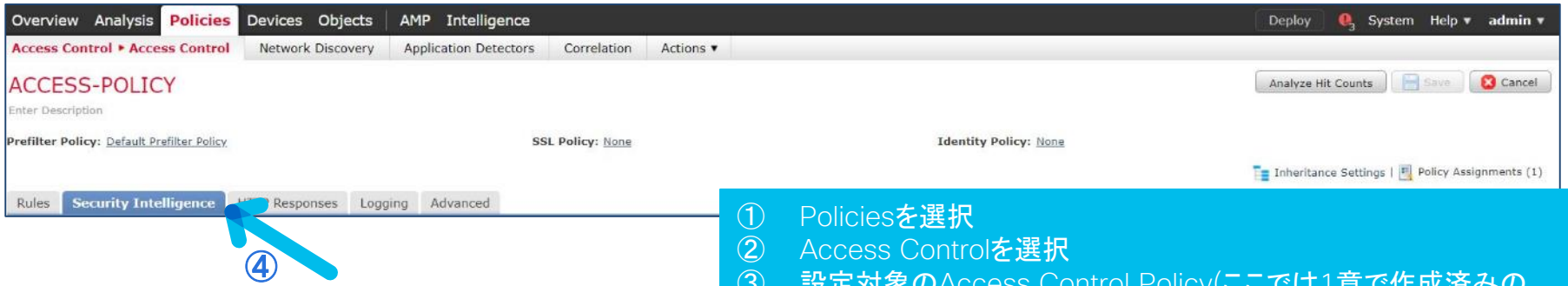
Security Intelligenceとは

- 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: Security Intelligence の設定

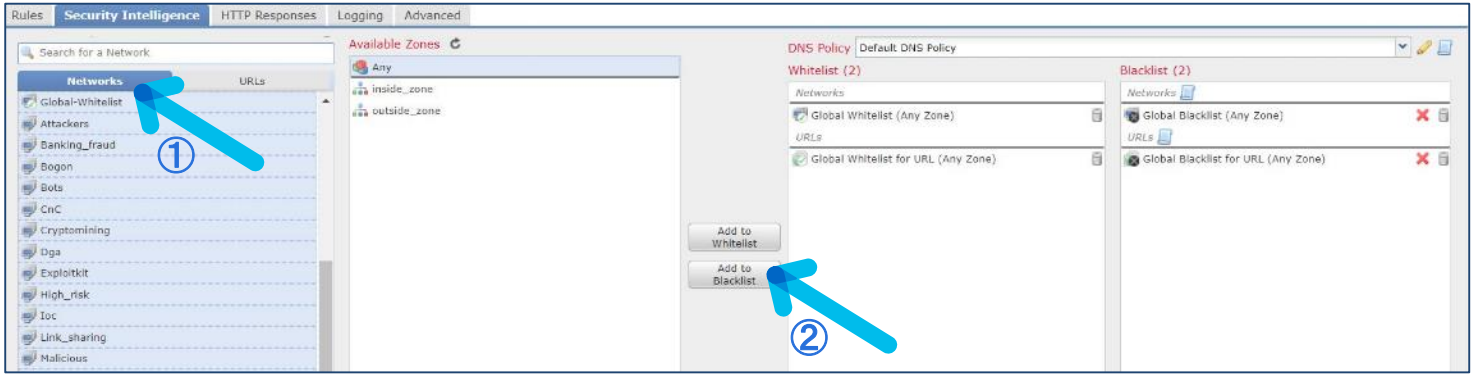
- Security Intelligenceにヒットした通信をブロックする設定を行う

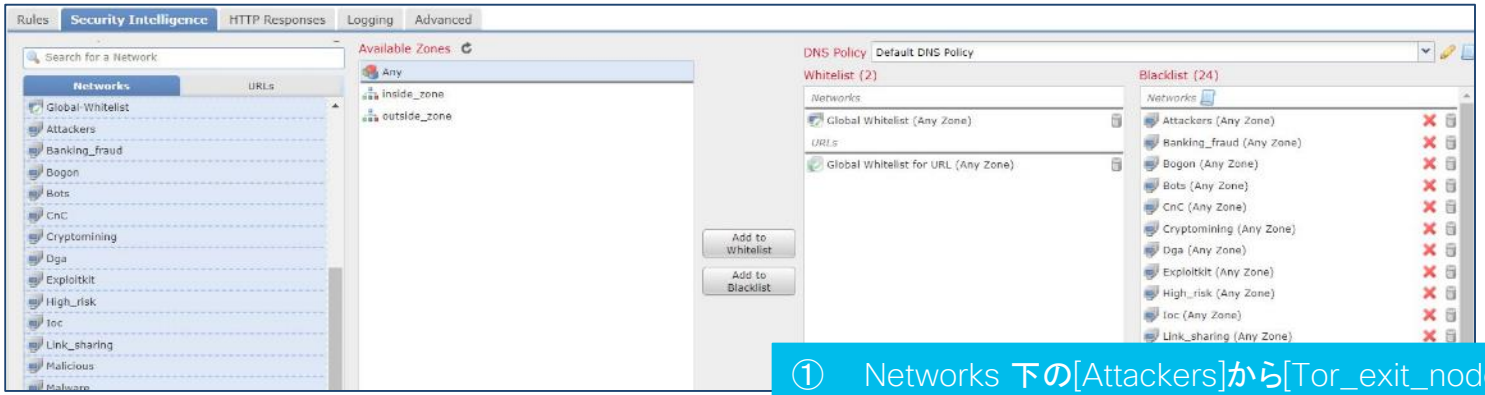




① Policiesを選択
② Access Controlを選択
③ 設定対象のAccess Control Policy(ここでは1章で作成済みの“ACCESS-POLICY”とする)の右側の鉛筆マークを選択
④ Security Intelligence を選択

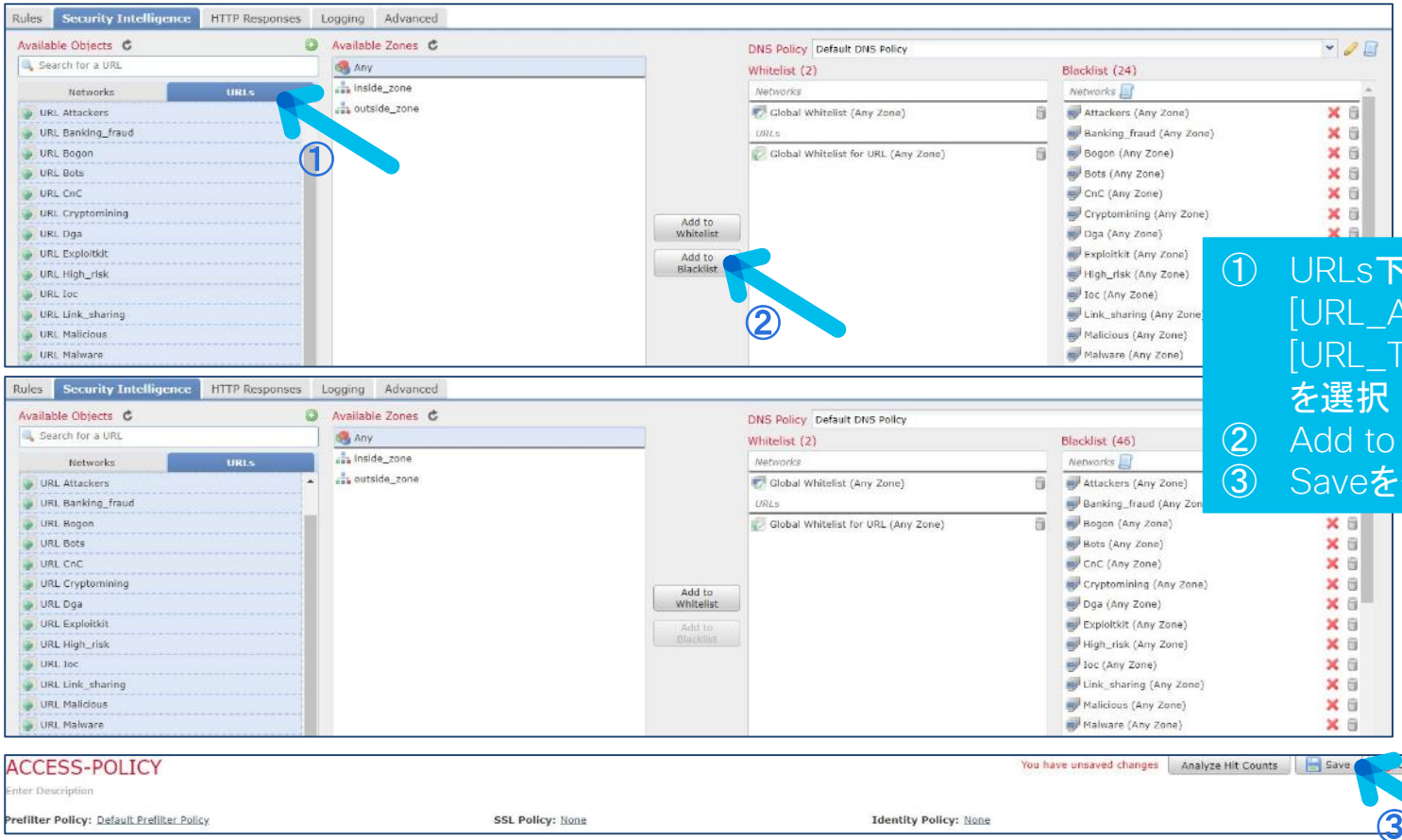
ステップ 1: Security Intelligence の設定 Network





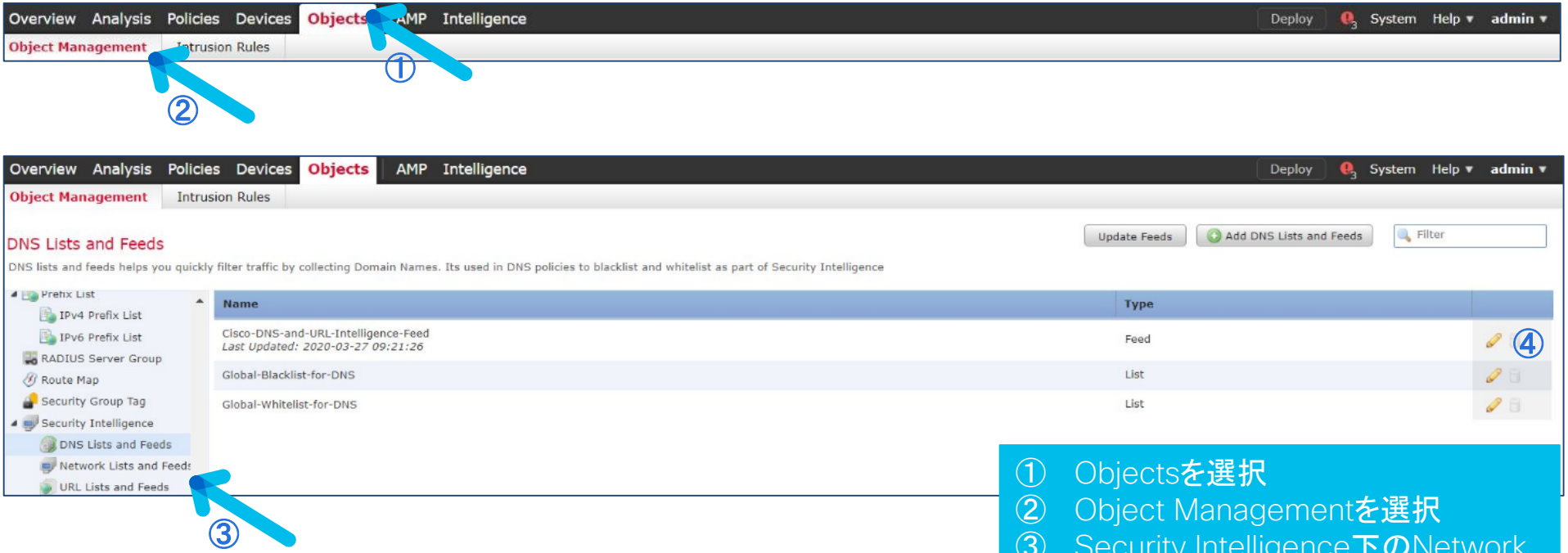
① Networks 下の[Attackers]から[Tor_exit_node]までを選択
② Add to Blacklist をクリック

ステップ 1: Security Intelligence の設定 URL



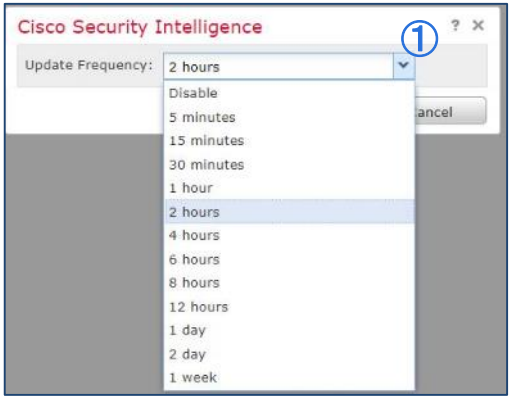
① URLs下の[URL_Attackers]から[URL_Tor_exit_node]までを選択
② Add to Blacklist をクリック
③ Saveをクリック

参考: Security Intelligence の更新頻度の変更①



① Objectsを選択
② Object Managementを選択
③ Security Intelligence下のNetwork Lists and Feeds を選択
④ Cisco-Intelligence-Feed 右側の鉛筆マークをクリック

参考: Security Intelligence の更新頻度の変更②

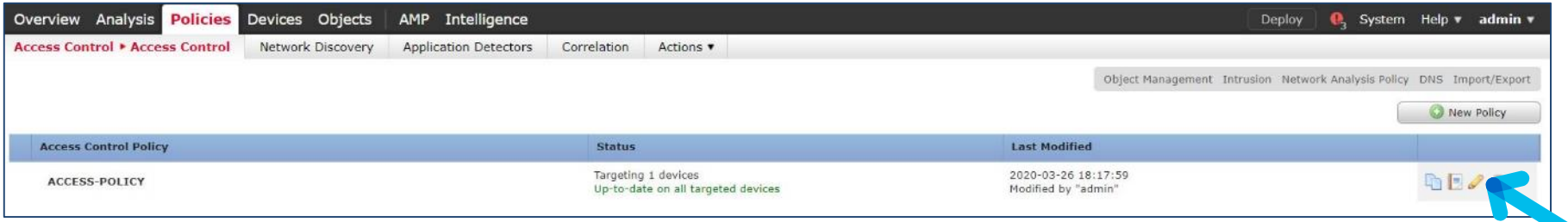


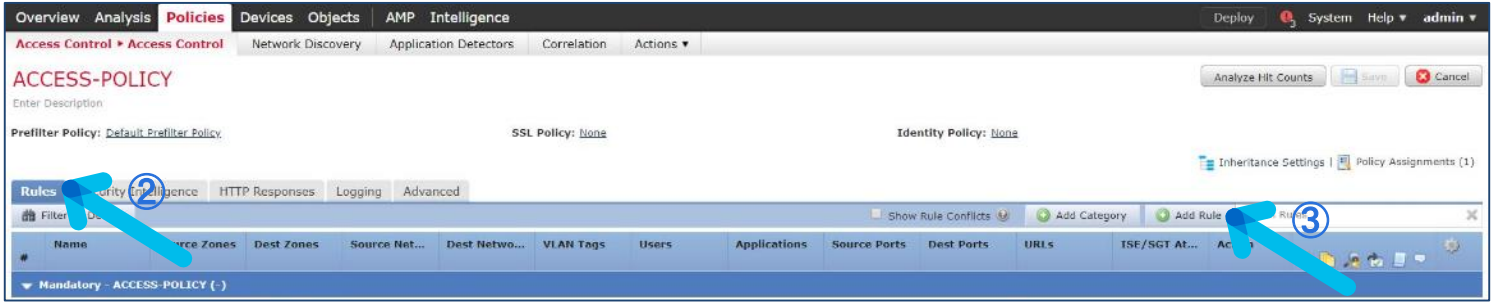
① Update Frequency のドロップダウンリストを開き、任意の更新頻度を選択

- デフォルト は2時間
- URL List の更新頻度は DNS Lists and Feeds から変更可能

ステップ 2: Access Rule の設定①

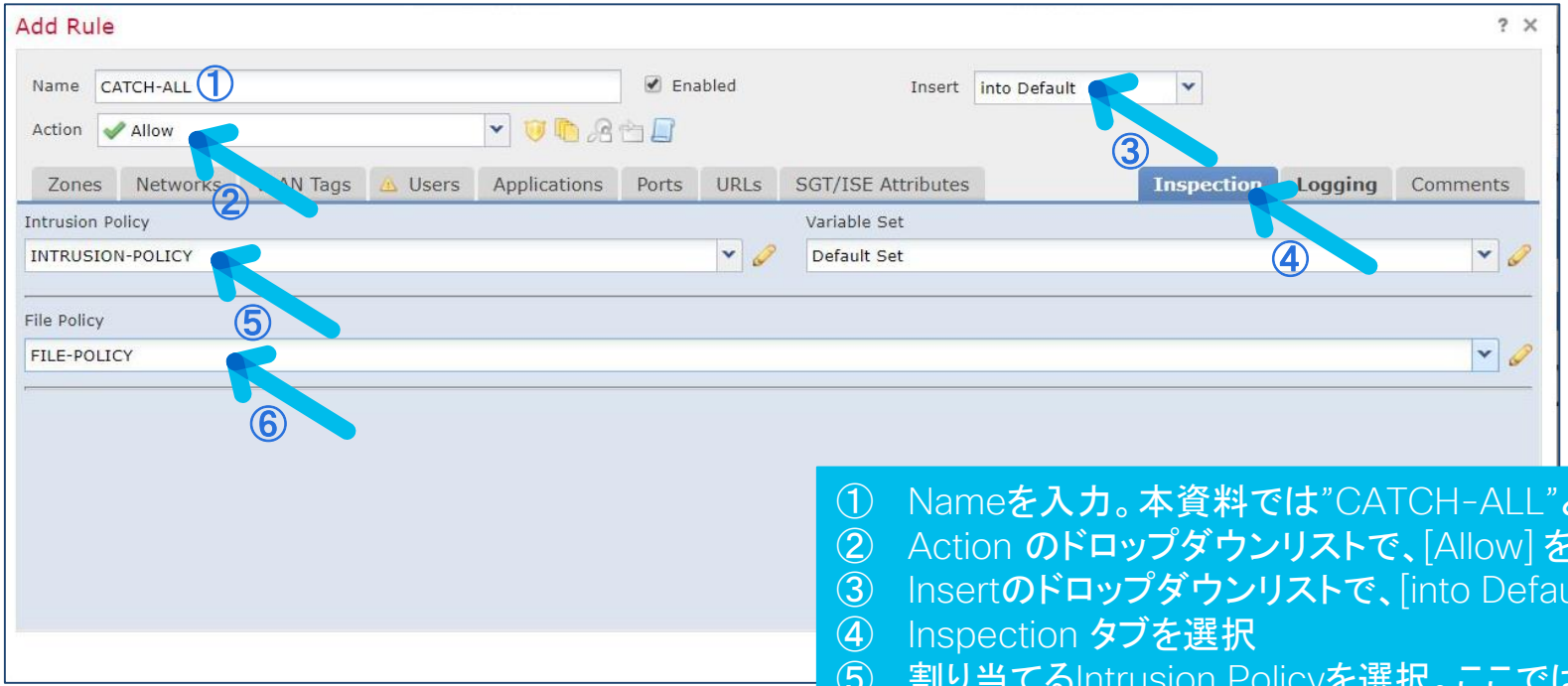
- 全ての通信をモニタするAccess Ruleを作成し、Intrusion PolicyとFile Policyを適用する





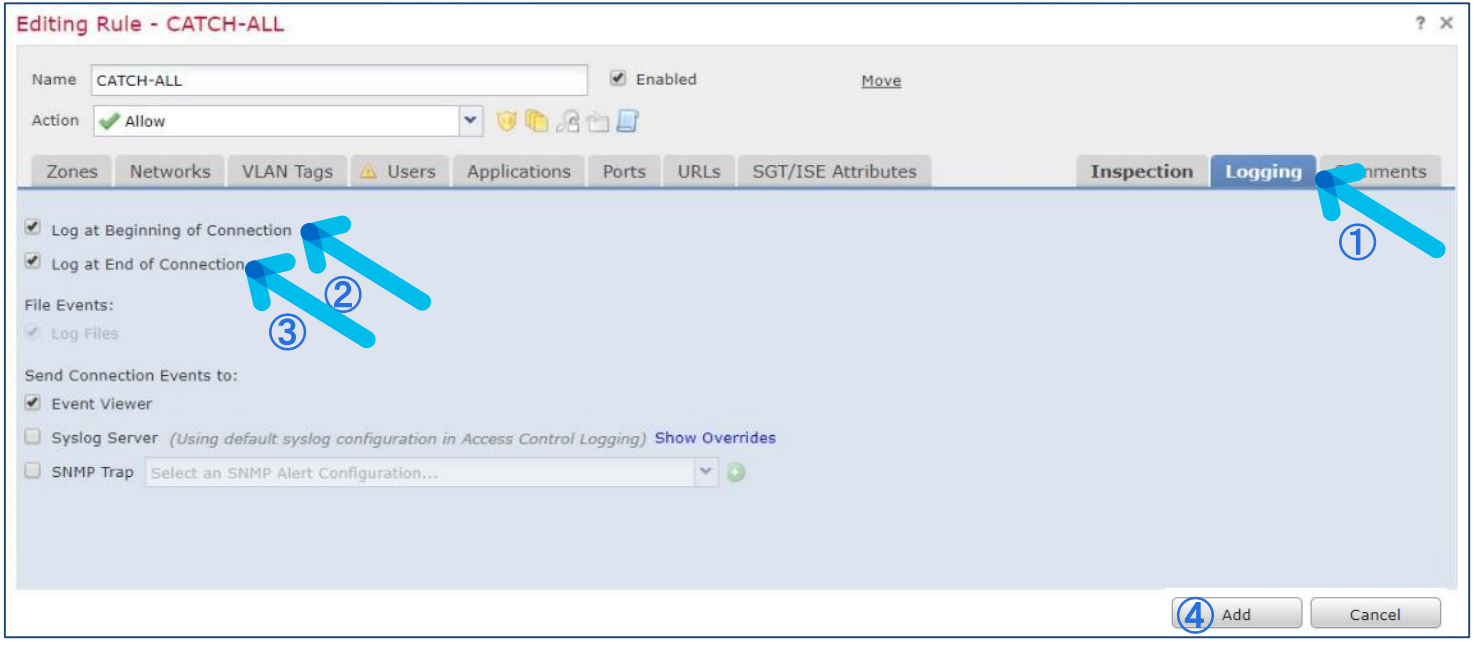
① Access Ruleを設定するAccess Control Policyを選択する。ここでは作成済みの[ACCESS-POLICY]とする
② Rules タブを選択
③ Add Rule を選択

ステップ 2: Access Rule の設定②



① Nameを入力。本資料では”CATCH-ALL”とする
② Action のドロップダウンリストで、[Allow] を選択
③ Insertのドロップダウンリストで、[into Default]を選択
④ Inspection タブを選択
⑤ 割り当てるIntrusion Policyを選択。ここでは作成済みの[INTRUSION-POLICY]を選択
⑥ 割り当てるFile Policyを選択。ここでは作成済みの[IFILE-POLICY]を選択

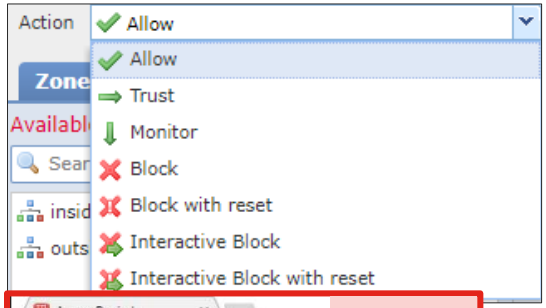
ステップ 2: Access Rule の設定③

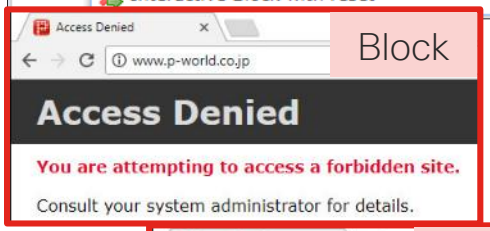


※Loggingの負荷が高い場合には②を省くことを推奨

① Logging タブを選択
② Log at Beginning of Connection にチェックを入れる
③ Log at End of Connectionにチェックを入れる
④ Add を選択

参考: Action のオプションについて

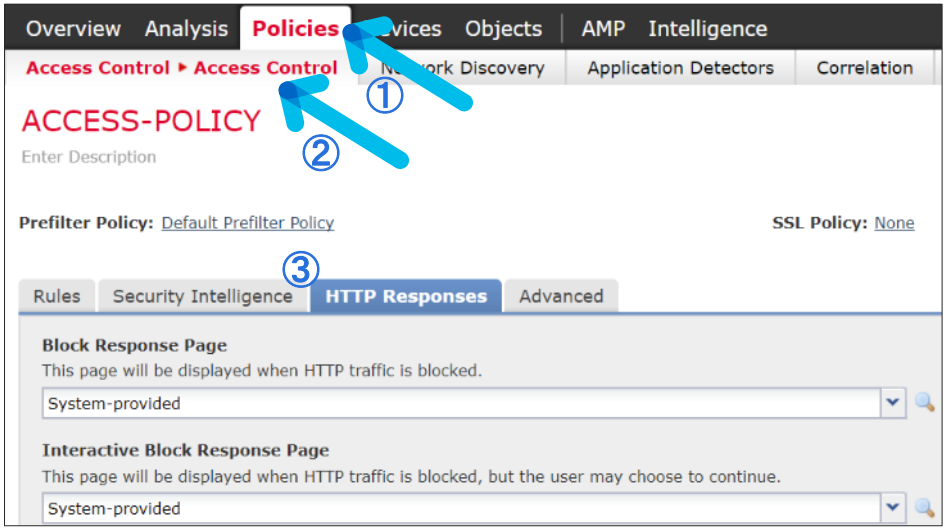


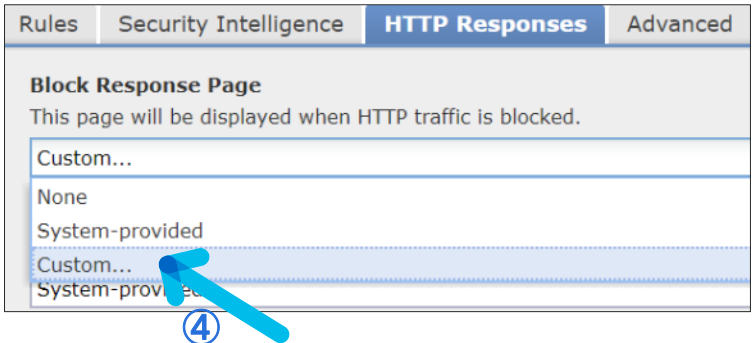


- FTD で使用できる Action は全 7 種
  - Allow: パケットを信頼せずに許可し、追加でIPSやAMPのチェックを実施することが可能
  - Trust: パケットを信頼して許可。IPSやAMPのチェックは不可
  - Monitor: ログを取るためだけに使用。トラフィックは次のルールに転送
  - Block: パケットを破棄
  - Block w/ reset: パケットを破棄すると同時に、送信元に対し、TCP RSTパケットを送信し、通信を即遮断
  - Interactive Block: ブロックが推奨されるユーザアクションに対し警告を行うが、ユーザの判断で通信し続けることも可能
  - Interactive Block w/ reset: 上記と同様。ただし、警告通りに通信をブロックする場合、送信元に対して TCP RST パケットを送信

Continue すれば、サイトへのアクセスが可能

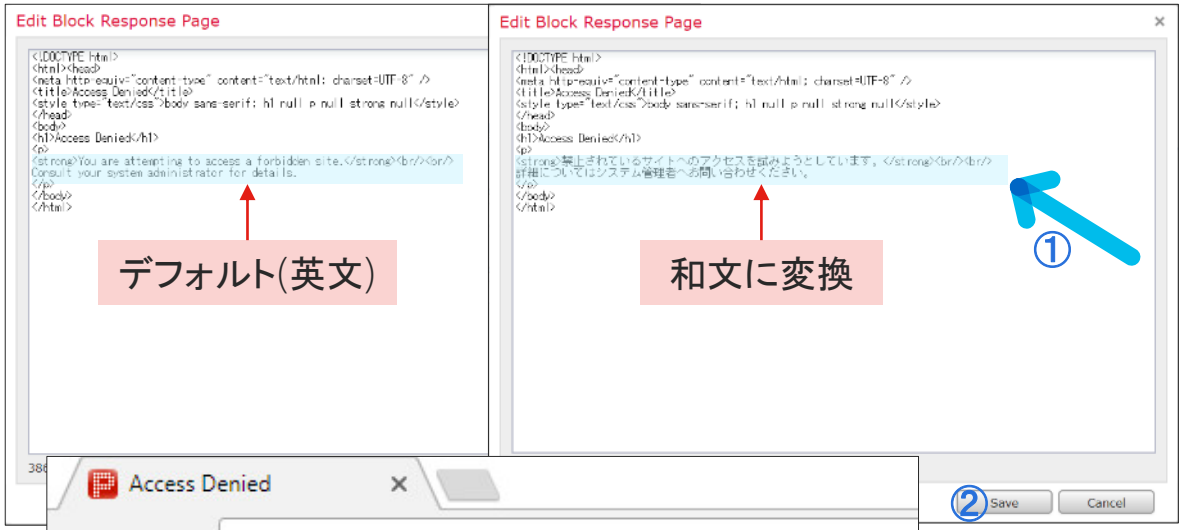
参考: Block 時のHTTP Response ページの編集①





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

参考: Block 時のHTTP Response ページの編集②

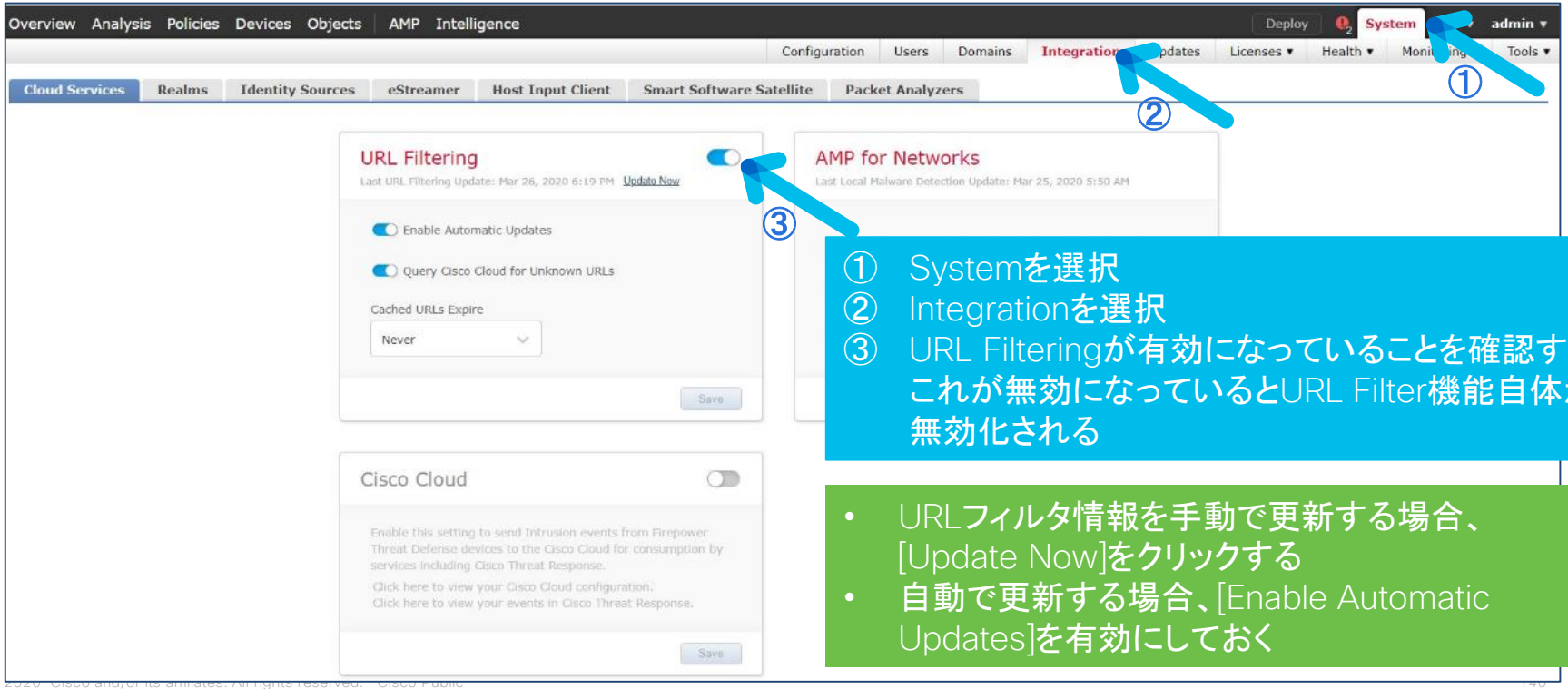


① 任意の文章に変更 (HTML形式)
② Save を選択

- アクセスページを表示させた結果
- レスポンスが和文になっている
- 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: URL Filter機能の有効化確認

- URL Filter機能自体が有効になっていることを確認する

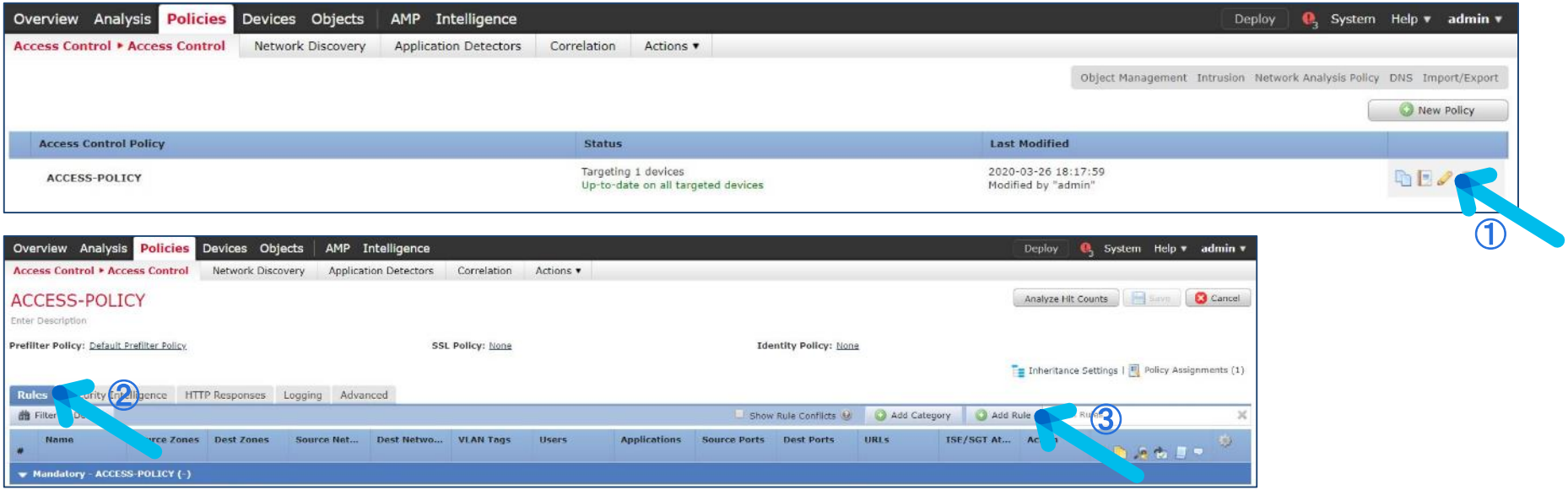


① Systemを選択
② Integrationを選択
③ URL Filteringが有効になっていることを確認する。これが無効になっているとURL Filter機能自体が無効化される

- URLフィルタ情報を手動で更新する場合、[Update Now]をクリックする
- 自動で更新する場合、[Enable Automatic Updates]を有効にしておく

ステップ 4: URL Category Monitor の設定①

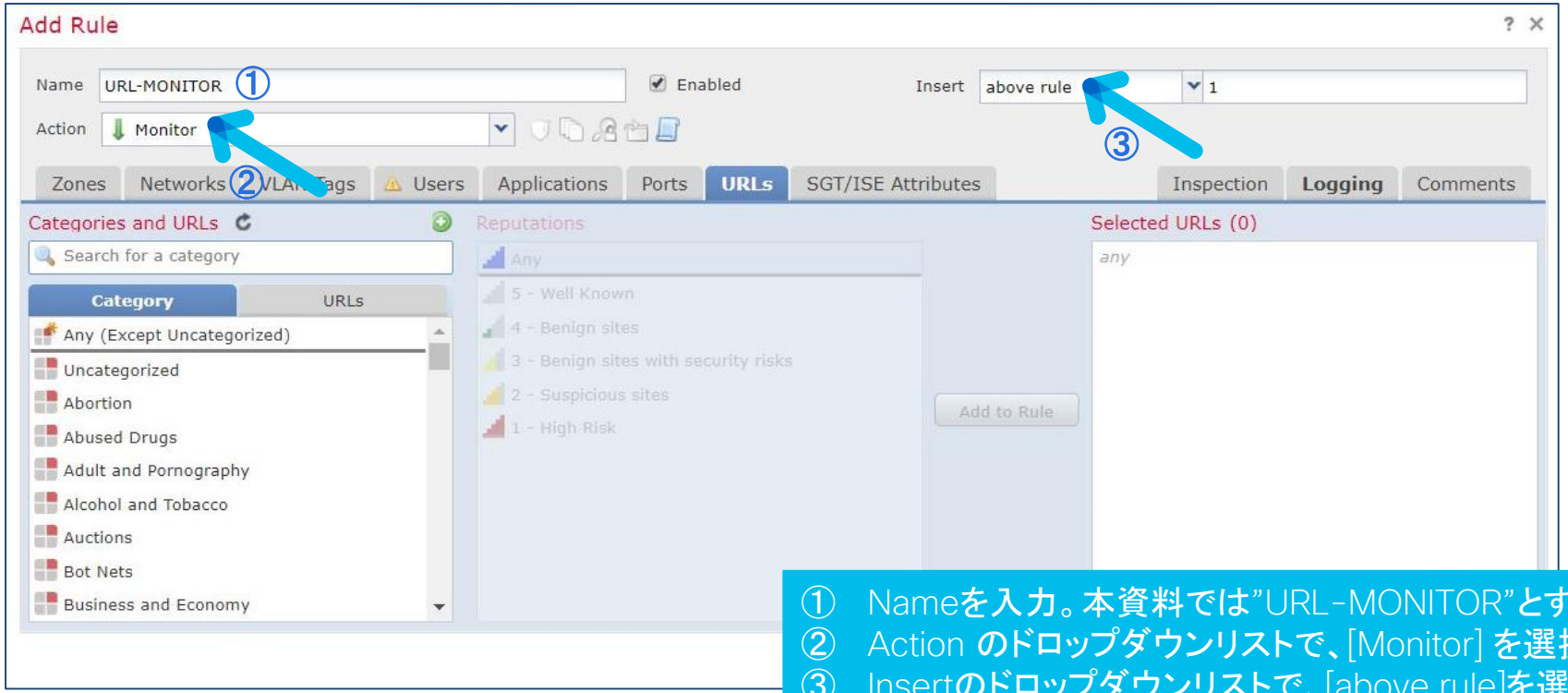
- 全ての通信に対し、URLカテゴリのロギングを行うRuleを追加



① Access Ruleを設定するAccess Control Policyを選択する。ここでは作成済みの[ACCESS-POLICY]とする
② Rules タブを選択
③ Add Rule を選択

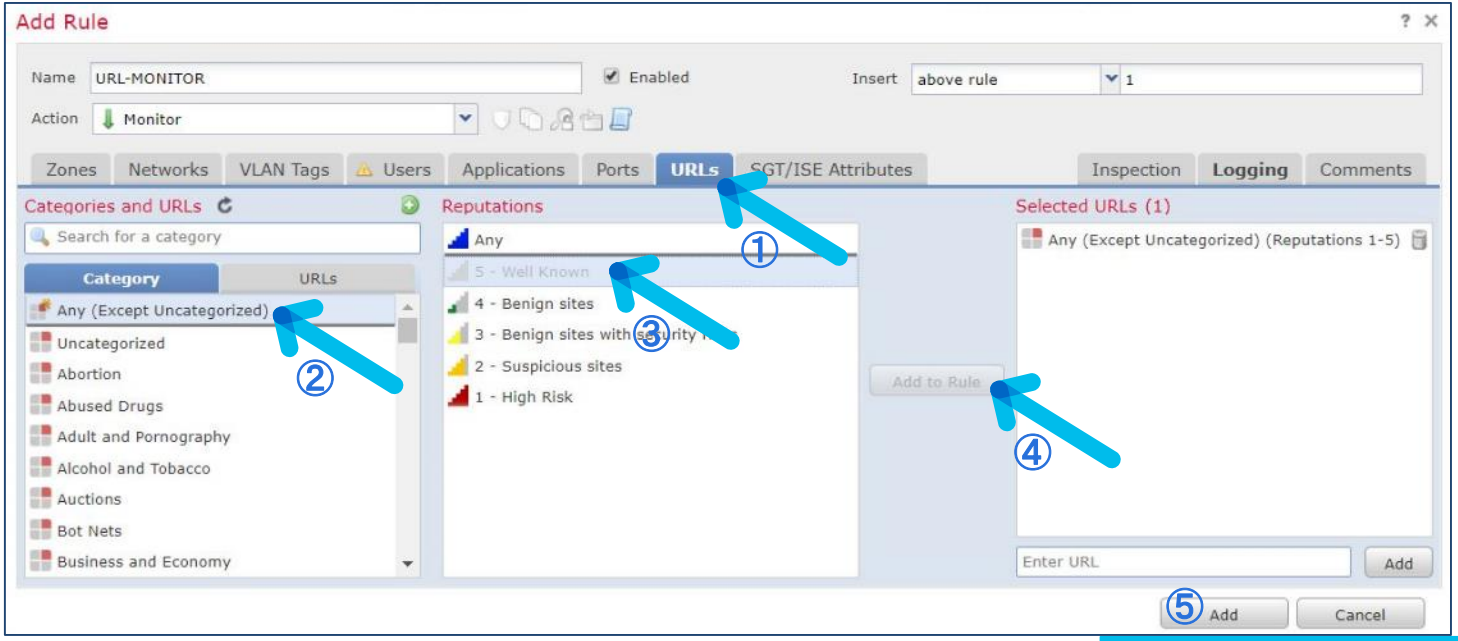
ステップ 4: URL Category Monitor の設定②

- 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 Nameを入力。本資料では"URL-MONITOR"とする
② Action のドロップダウンリストで、[Monitor] を選択
③ Insertのドロップダウンリストで、[above rule]を選択

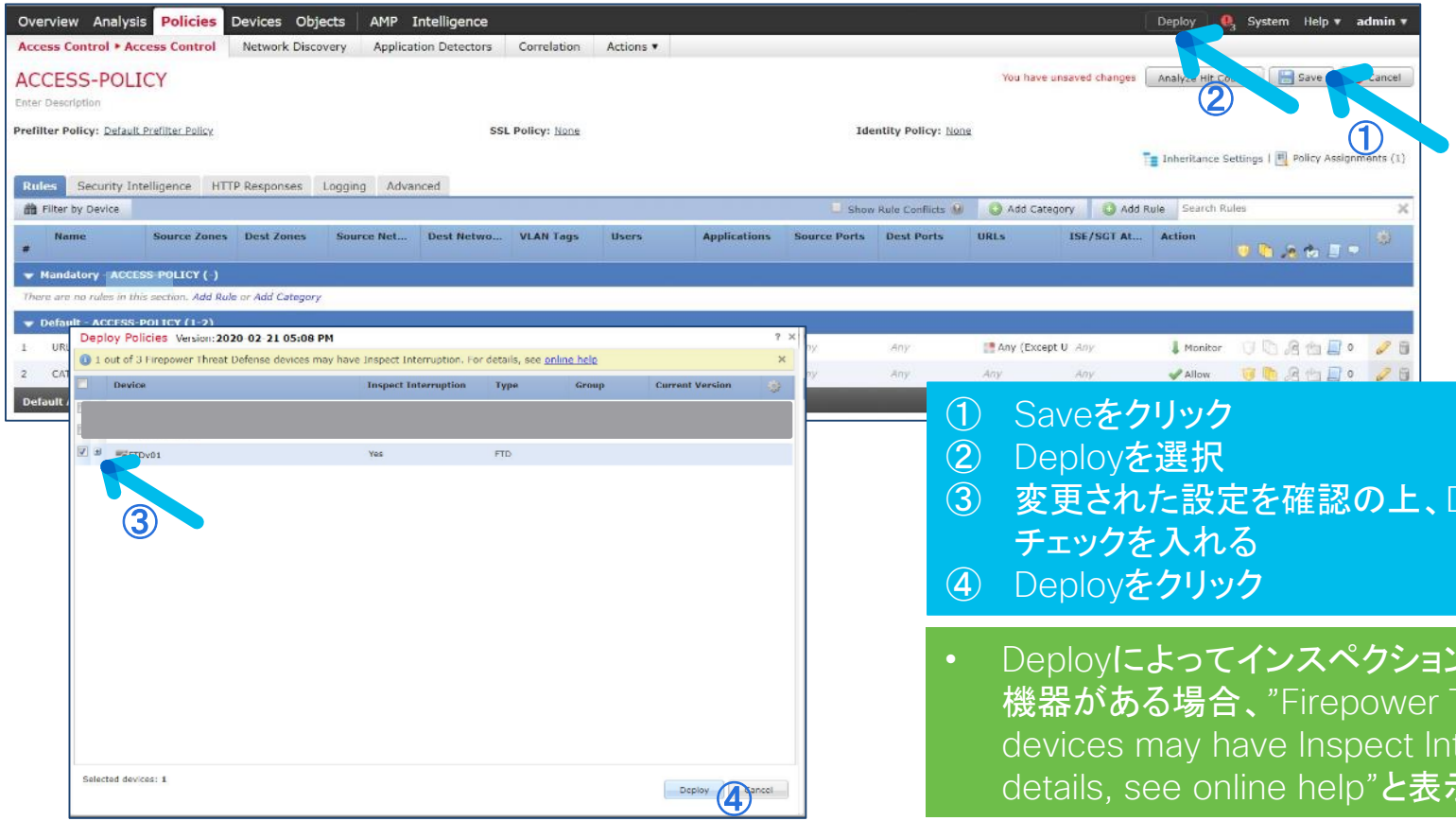
ステップ 4: URL Category Monitor の設定③



※Action：Monitorの場合、Loggingは自動的に設定される

① URLs タブを選択
② Any (Except Uncategorized) を選択
③ Reputations: 5 – Well Known を選択
④ Add to Rule をクリック
⑤ Addをクリック

ステップ 5:Access Control Policy保存

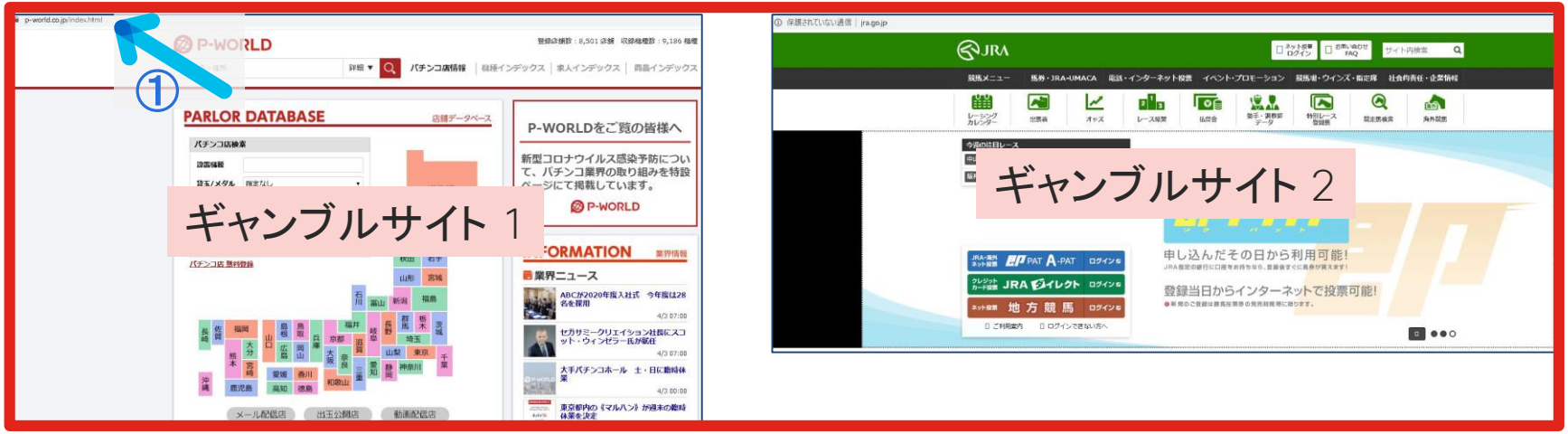


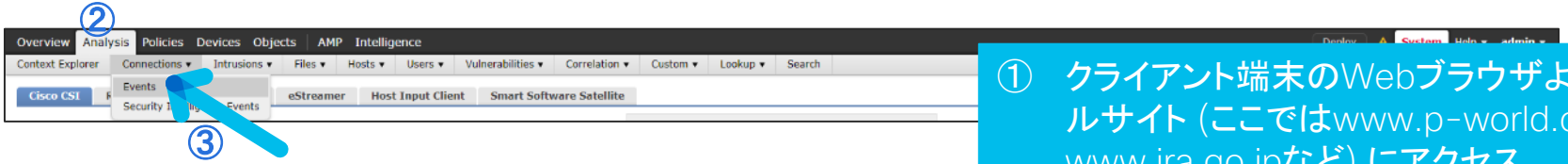
① Saveをクリック
② Deployを選択
③ 変更された設定を確認の上、Deploy対象機器にチェックを入れる
④ Deployをクリック

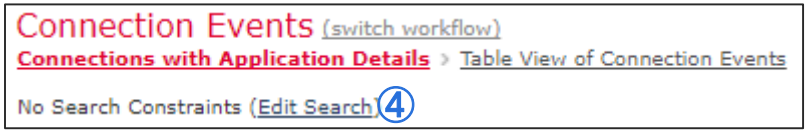
- Deployによってインスペクション処理に影響の出る機器がある場合、”Firepower Threat Defense devices may have Inspect Interruption. For details, see online help”と表示される

ステップ 6: URL Filter のテスト①

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

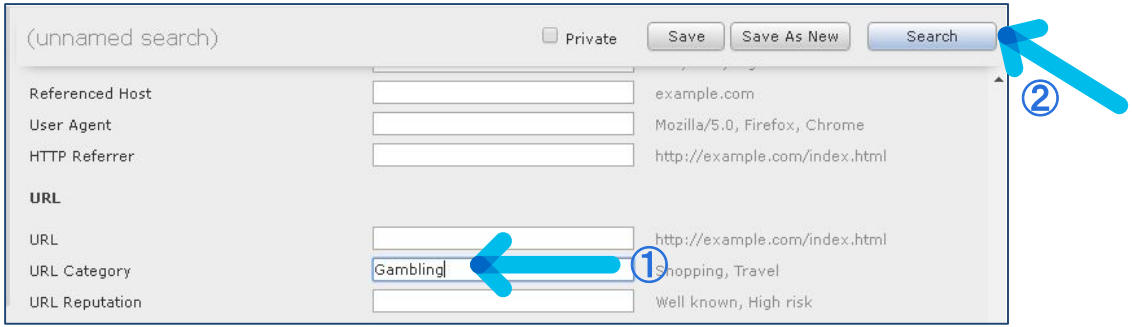






① クライアント端末のWebブラウザよりギャンブルサイト（ここではwww.p-world.co.jp、www.jra.go.jpなど）にアクセス
② Analysisタブを選択
③ Connections下のEventsを選択
④ Edit Search をクリック

ステップ 6: URL Filter のテスト②



① URL: URL Category の欄に [Gambling] と入力
② Search をクリック

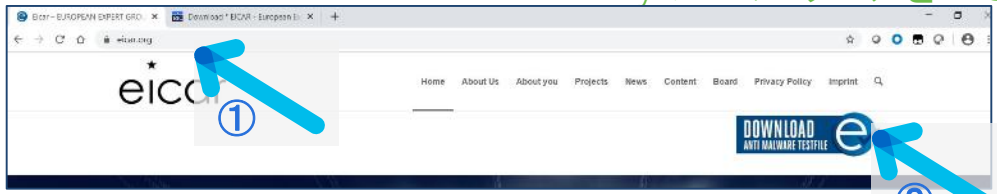
ステップ 6: URL Filter のテスト③

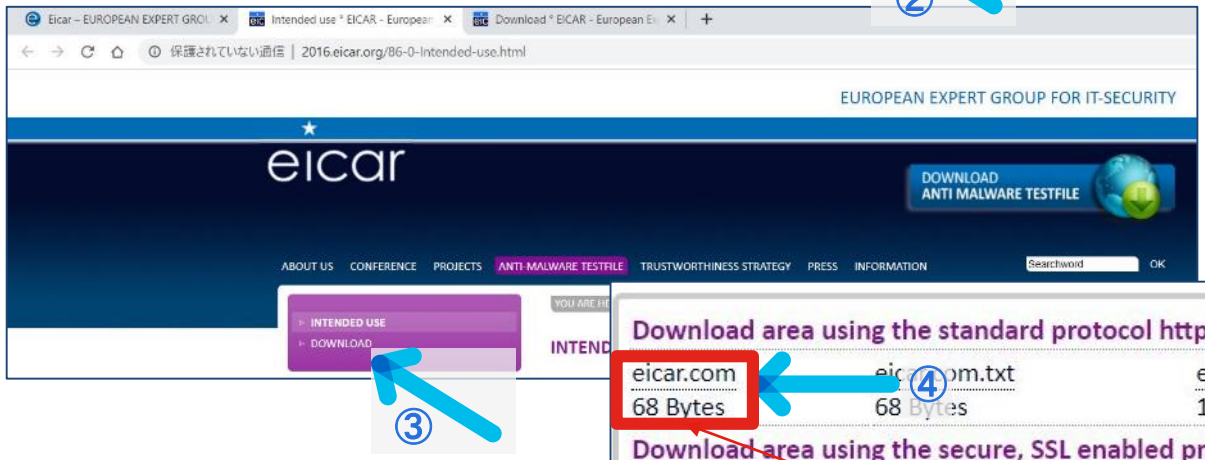
① ギャンブルサイトがURL CategoryでGambling へカテゴライズされていることを確認

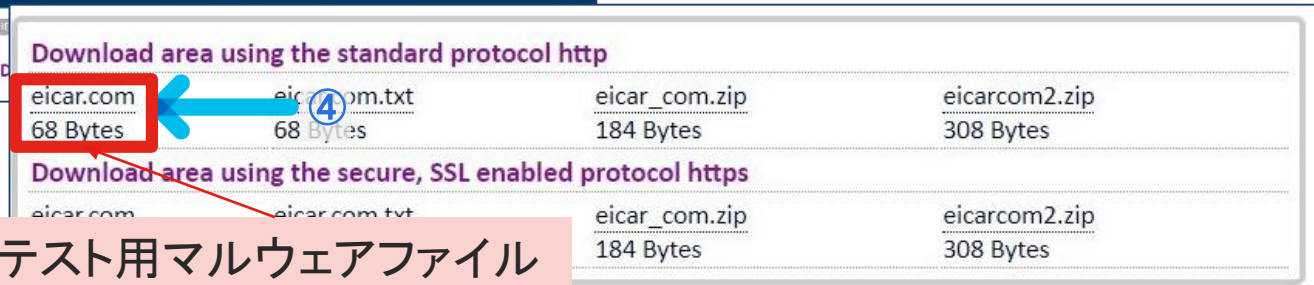
①

ステップ 7: AMP (File Policy) のテスト①

本テストでは、テスト用のマルウェアファイルをクライアント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



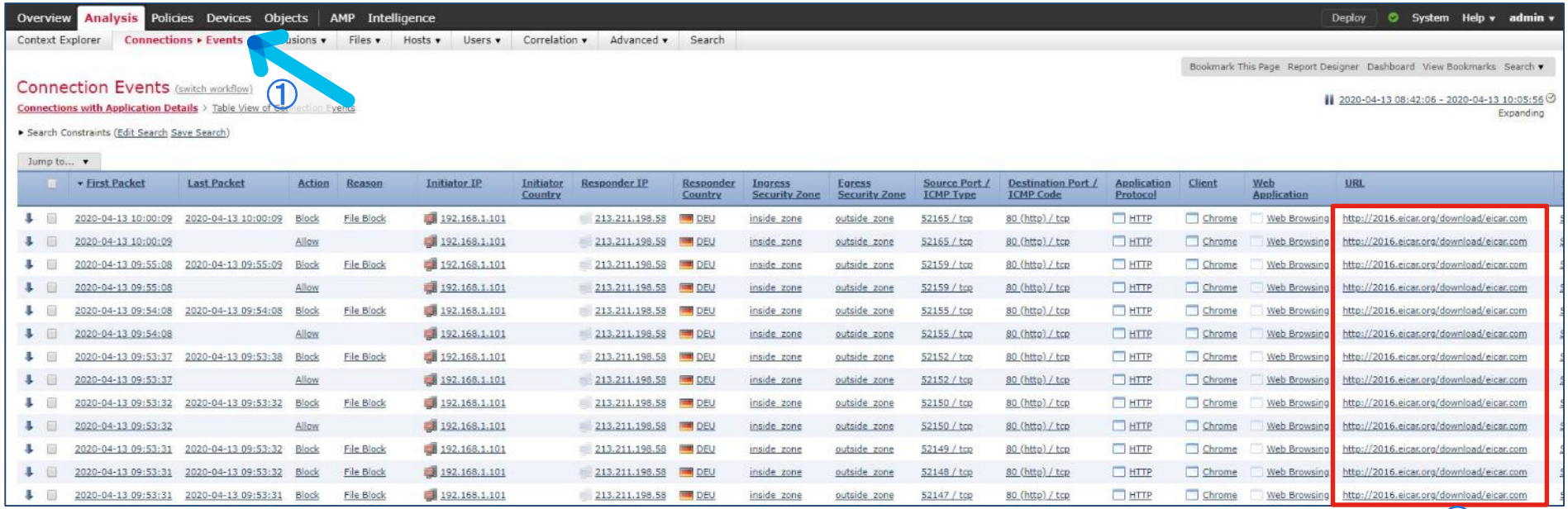




テスト用マルウェアファイル

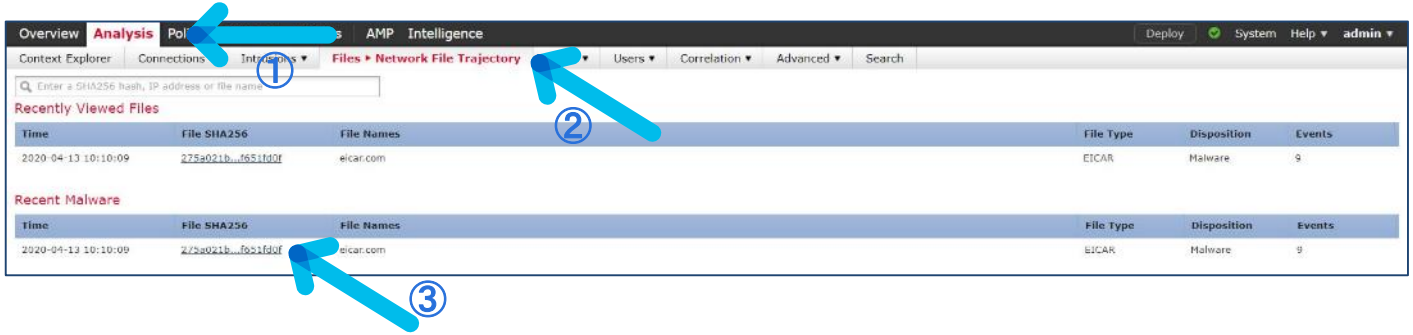
① クライアント端末のWebブラウザよりwww.eicar.org にアクセス
② [DOWNLOAD ANTI MALWARE TESTFILE]をクリック
③ [DOWNLOAD]をクリック
④ [eicar.com]をクリック。テスト用のマルウェアがダウンロードされる

ステップ 7: AMP (File Policy) のテスト②



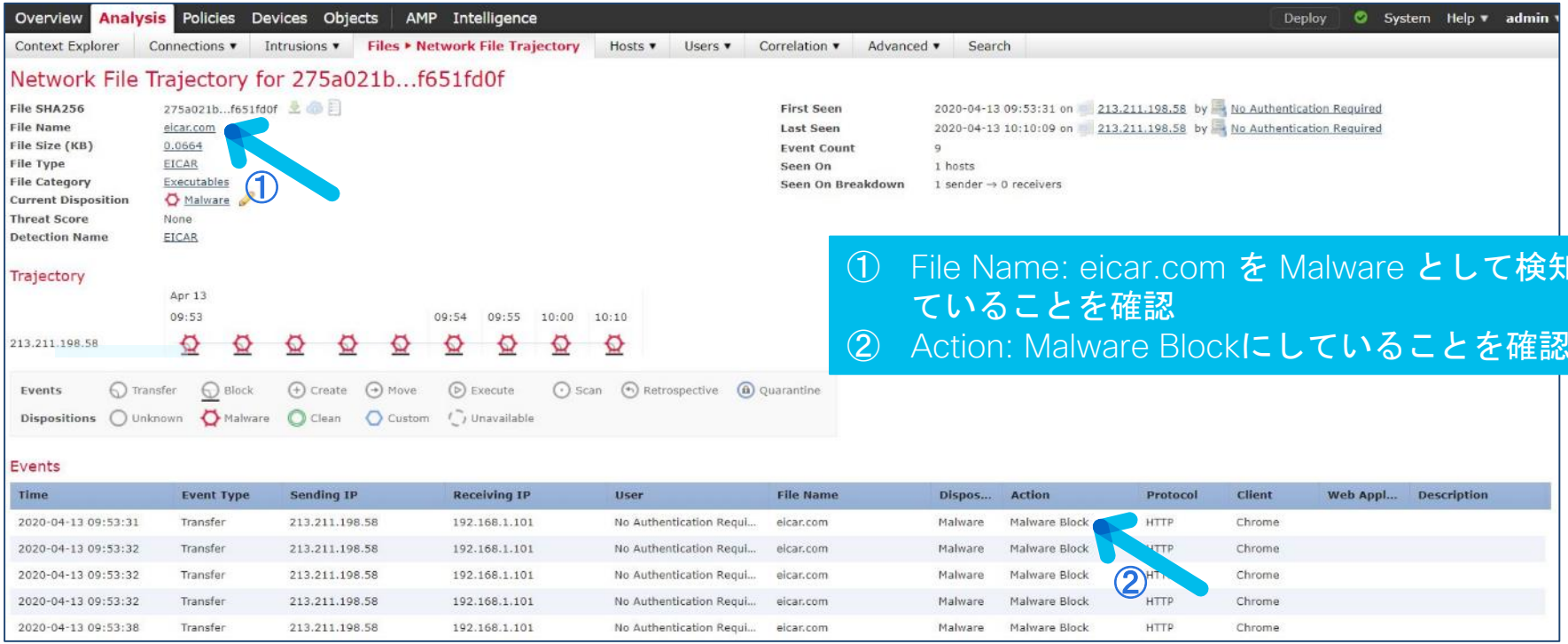
① Analytics > Connections > Events を選択
② eicar.org のログを確認

ステップ 7: AMP (File Policy) のテスト③



① Analysis を選択
② Files > Network File Trajectory を選択
③ File SHA256 の欄のハッシュ値をクリック

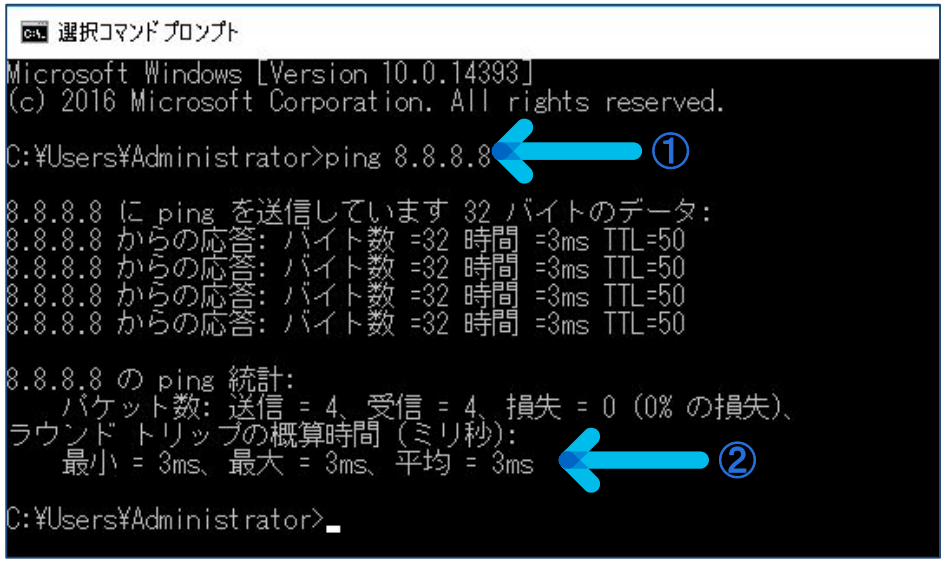
ステップ 7: AMP (File Policy) のテスト④



① File Name: eicar.com を Malware として検知していることを確認
② Action: Malware Blockにしていることを確認

ステップ 8: IPS (Intrusion Policy) のテスト①

本テストでは、クライアント端末よりpingコマンドを実行し、
テスト用に有効化したシグネチャ” PROTOCOL-ICMP PING (1:384:8)”によって
Intrusion Policy が攻撃を正しく検出できるかを確認する



① クライアント端末のWebブラウザより cmdを起動し、pingコマンドを実行。 宛先はFTDデバイスを経由した先の IPアドレスを使用すること。
② コマンドが終了することを確認する。

- 作成済みのIntrusion Policyの[Drop when Inline]が無効になっているため、パケットは破棄されずにpingコマンドによる疎通が可能。

ステップ 8: IPS (Intrusion Policy) のテスト②

① Analysis を選択
② Intrusions > Eventsを選択
③ PROTOCOL-ICMP PING (1:384:8)により攻撃が検出されていることを確認
④ Message(③)をクリックすることで該当する攻撃の詳細を確認可能。送信元/先IPアドレス、インパクトフラグなど

10. TLS Decryptionの設定

TLS 暗号化アクセラレーション

FTD は MITM (Man In The Middle) の形で通信を復号し、インスペクション後にまた通信を暗号化する
i.e. SSL/TLS アクセラレータではない
(クリアテキストのままオリジンサーバにパケットを送らない)

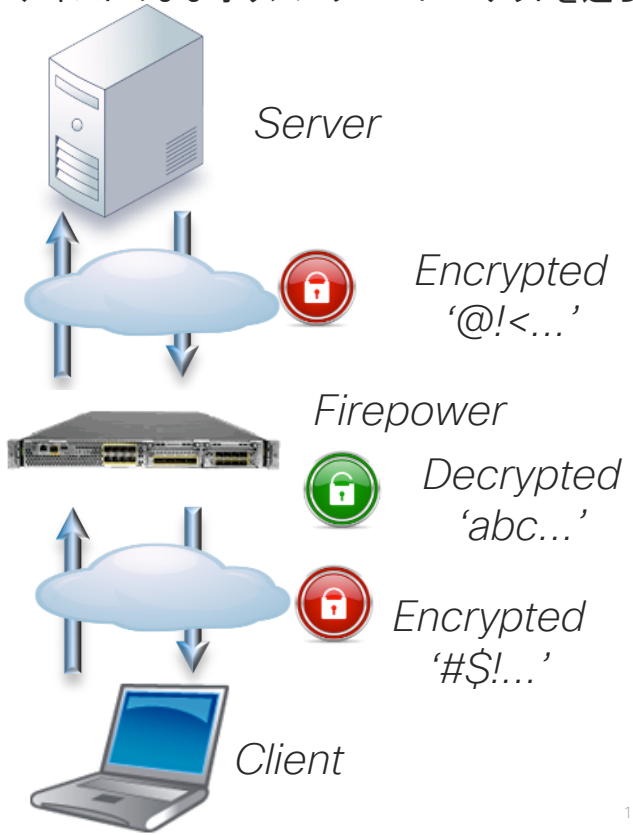
- SSL/TLS で暗号化された通信を復号してインスペクションを行う機能
  - inbound inline (L1), transparent (L2), routed (L3)

    → Decrypt – Known Key 設定を利用

    → 主に不特定多数の端末から自身が管理している公開サーバへの通信を復号 (主に IPS として利用される場合が多い)
  - outbound inline (L1), transparent (L2), routed (L3)

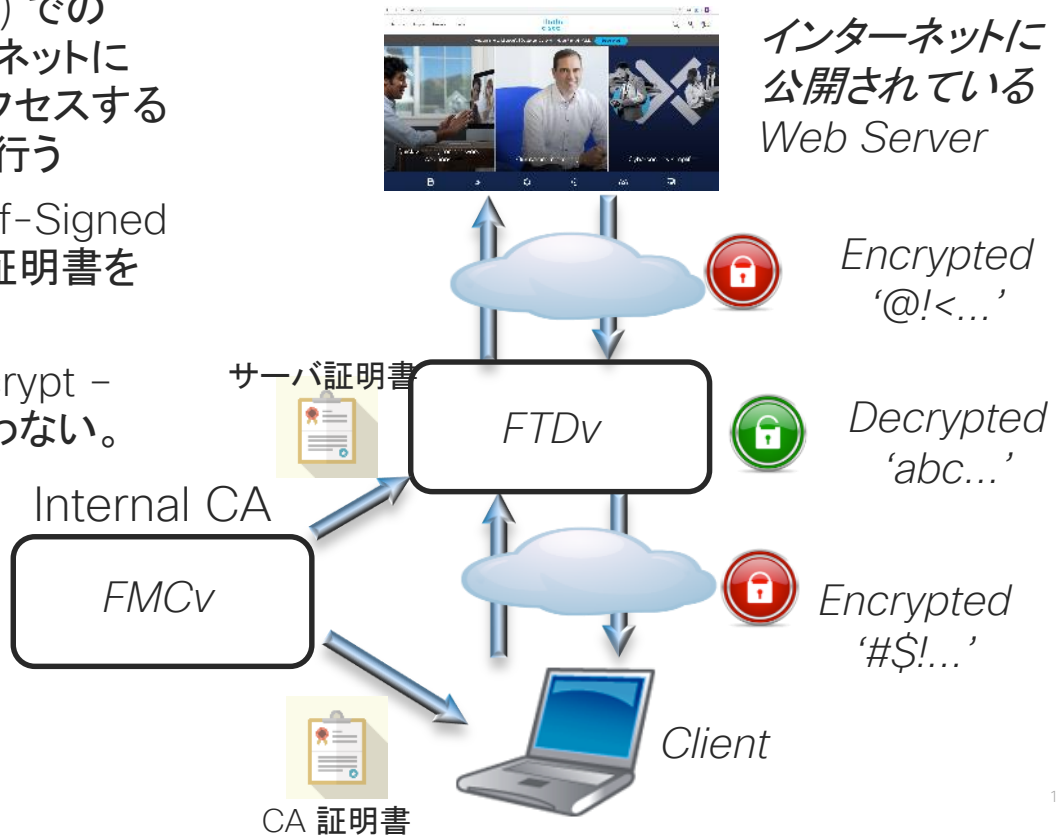
    → Decrypt – Resign 設定を利用

    → 主に自身が管理しているネットワーク内から不特定多数の公開サーバへの通信を復号 (主に NGFW として利用される場合が多い)
- FP2k,4k,9k はハードウェア処理による復号が可能。とはいえ、コネクション確立等はソフトウェア処理であり、負荷は高い。詳しくはデータシート参照
- その他のモデルではすべてソフトウェア処理となり、90%以上のパフォーマンス劣化があるため、利用には注意が必要
- Inline TAP, passive interfaceでは未サポート

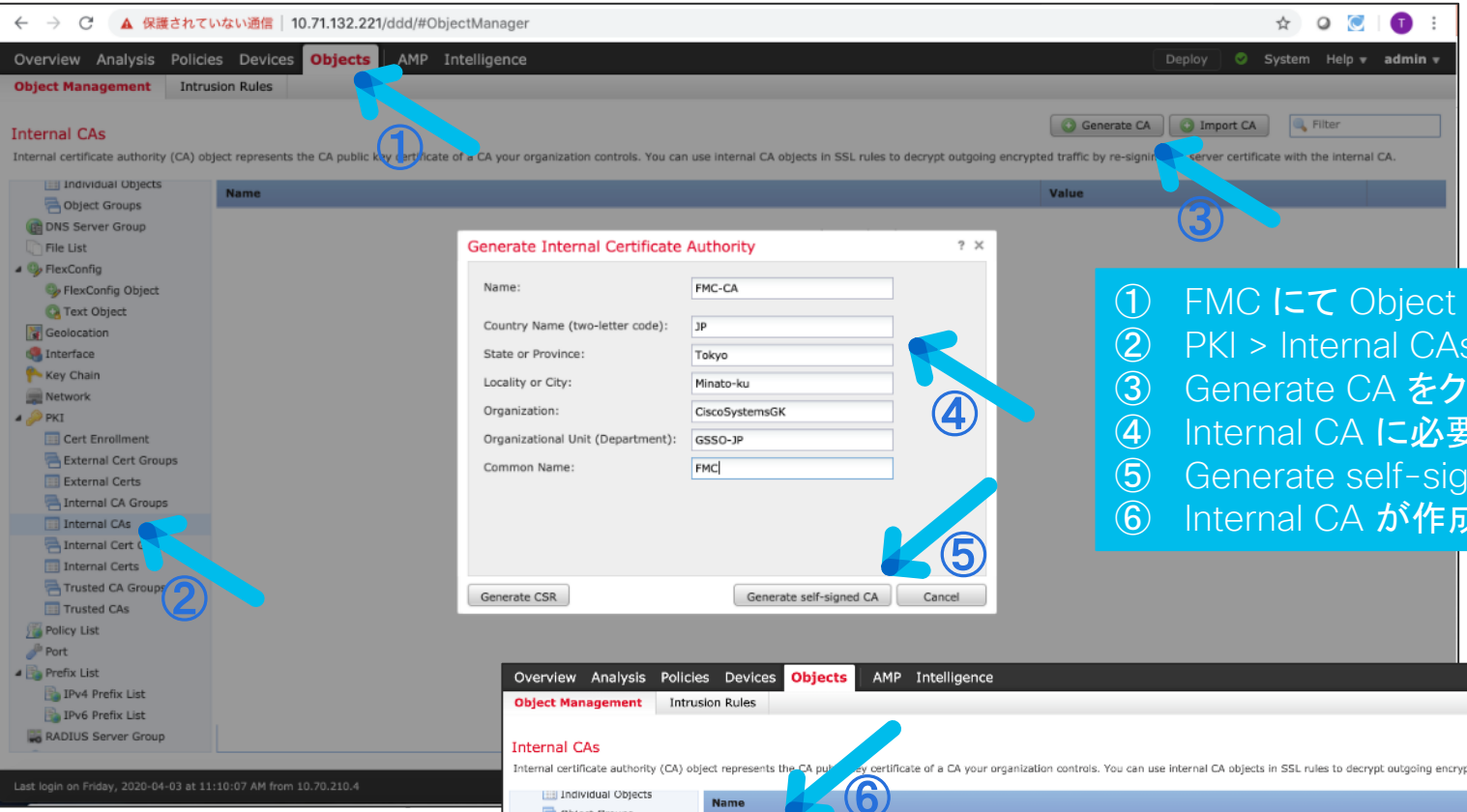


このガイドでのシナリオ

- Outbound (i.e. Decrypt – Resign) での TLS 復号を FTD で行い、インターネットに公開されている Web サーバにアクセスする際に、FTD でのインスペクションを行う
- 簡素化のため、Internal CA を Self-Signed で FMC にて立ち上げ、その CA 証明書をクライアントにインストールする
- このガイドでは、Inbound (i.e. Decrypt – Known Key) での TLS 復号は行わない。



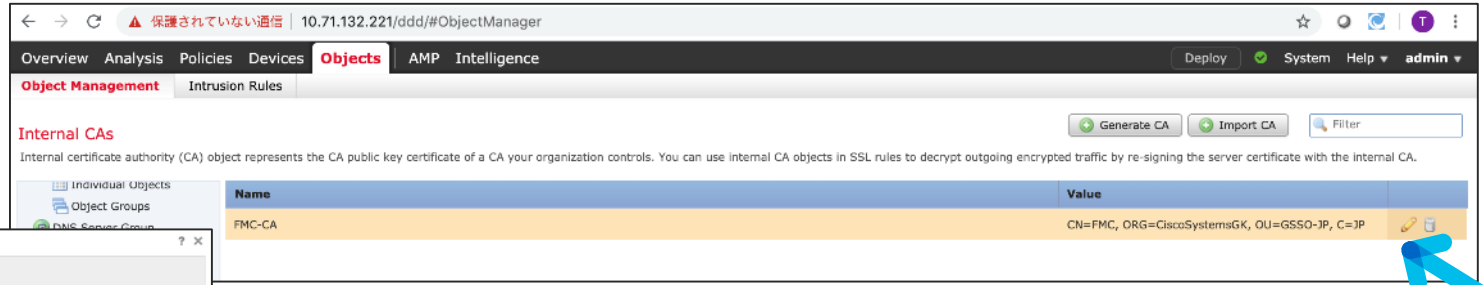
ステップ1-1: FMC での Internal CA 作成

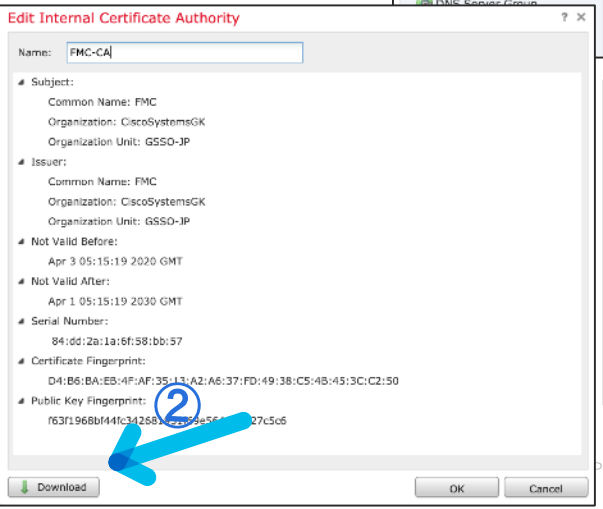


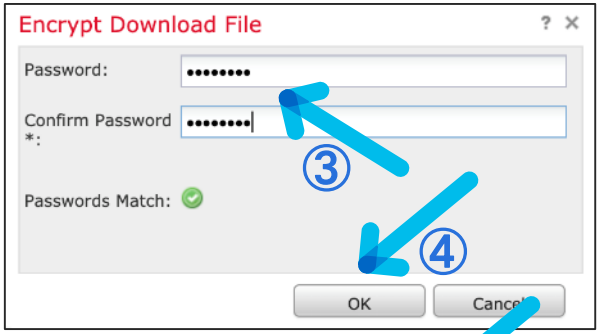
① FMC にて Object を選択
② PKI > Internal CAs を選択
③ Generate CA をクリック
④ Internal CA に必要なパラメータを埋める
⑤ Generate self-signed CA をクリック
⑥ Internal CA が作成される

ステップ2-1: Internal CA の証明書を入手

テスト PC は FMC の Internal CA を信頼する必要があるため、Internal CA の証明書をテスト PC の「信頼されたルート証明機関」にインポートする。そのためにまずは Internal CA の PKCS #12 形式のファイルを入手する





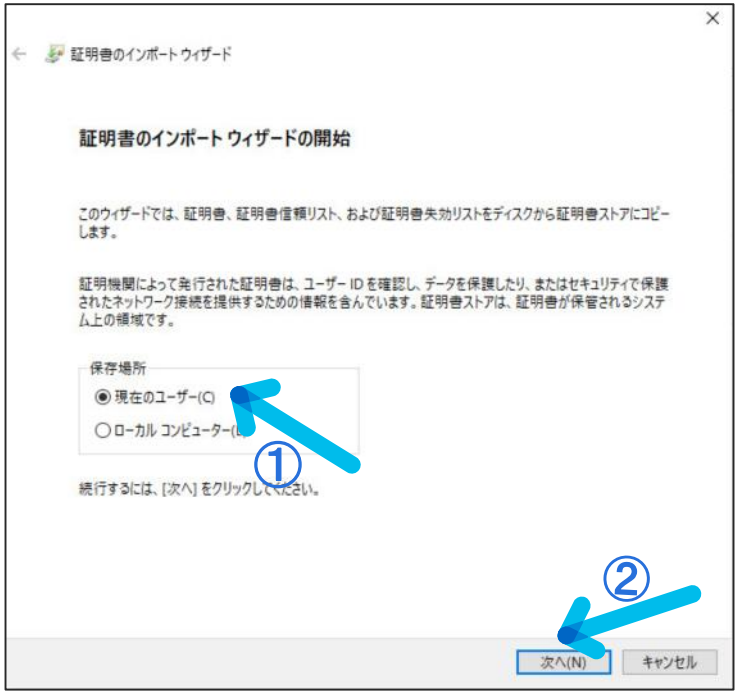


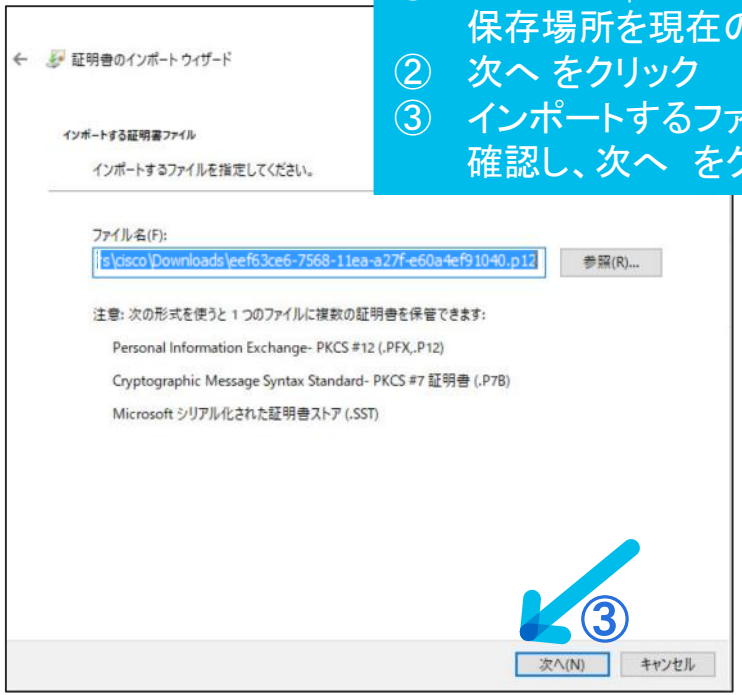
① 作成した Internal CA の Edit (鉛筆アイコン) をクリック
② Download をクリック
③ PKCS #12 ファイルのパスワードを設定
④ OK をクリック
⑤ PKCS #12 ファイルがダウンロードされる

ステップ2-2: PC への Internal CA 証明書のインポート(参考)(続き)

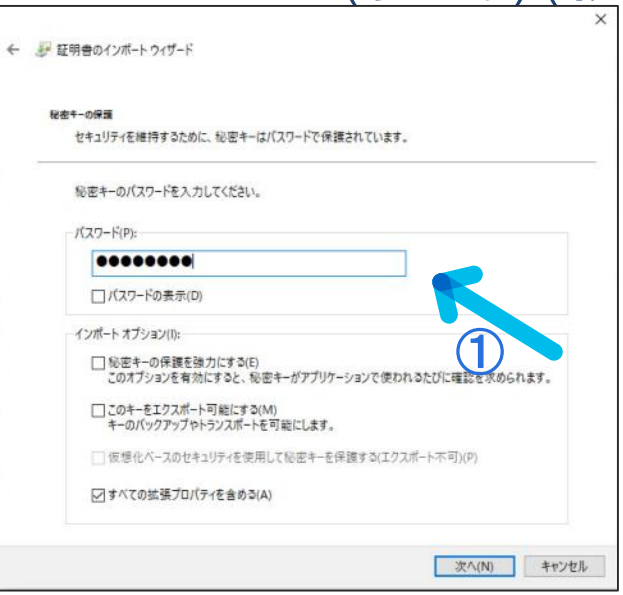
入手した Internal CA の PKCS #12 形式のファイルを、テスト PC にコピーし、インポートする。ここでは Windows 10 でのインポート手順を参考として記載

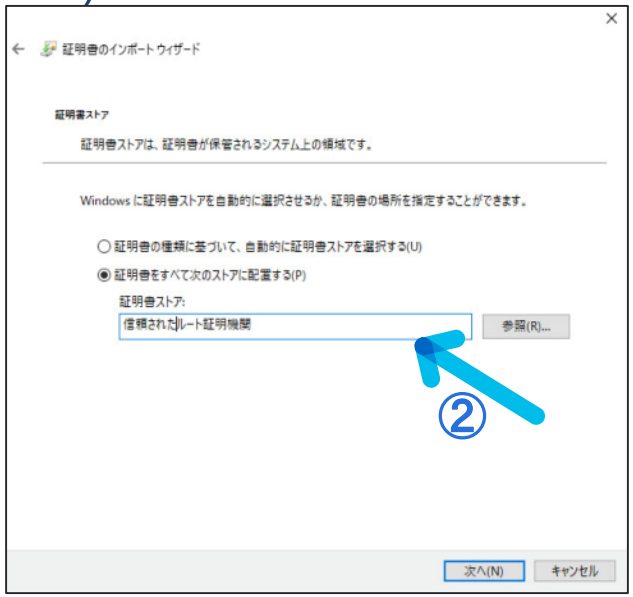
① 入手した .p12 ファイルをダブルクリックし、保存場所を現在のユーザーとする
② 次へ をクリック
③ インポートするファイルが合っていることを確認し、次へ をクリック

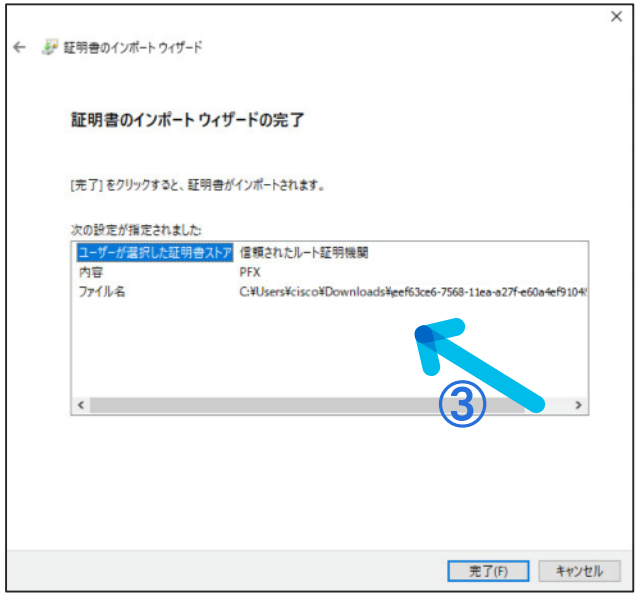




ステップ2-3: PC への Internal CA 証明書のインポート(参考)(続き)

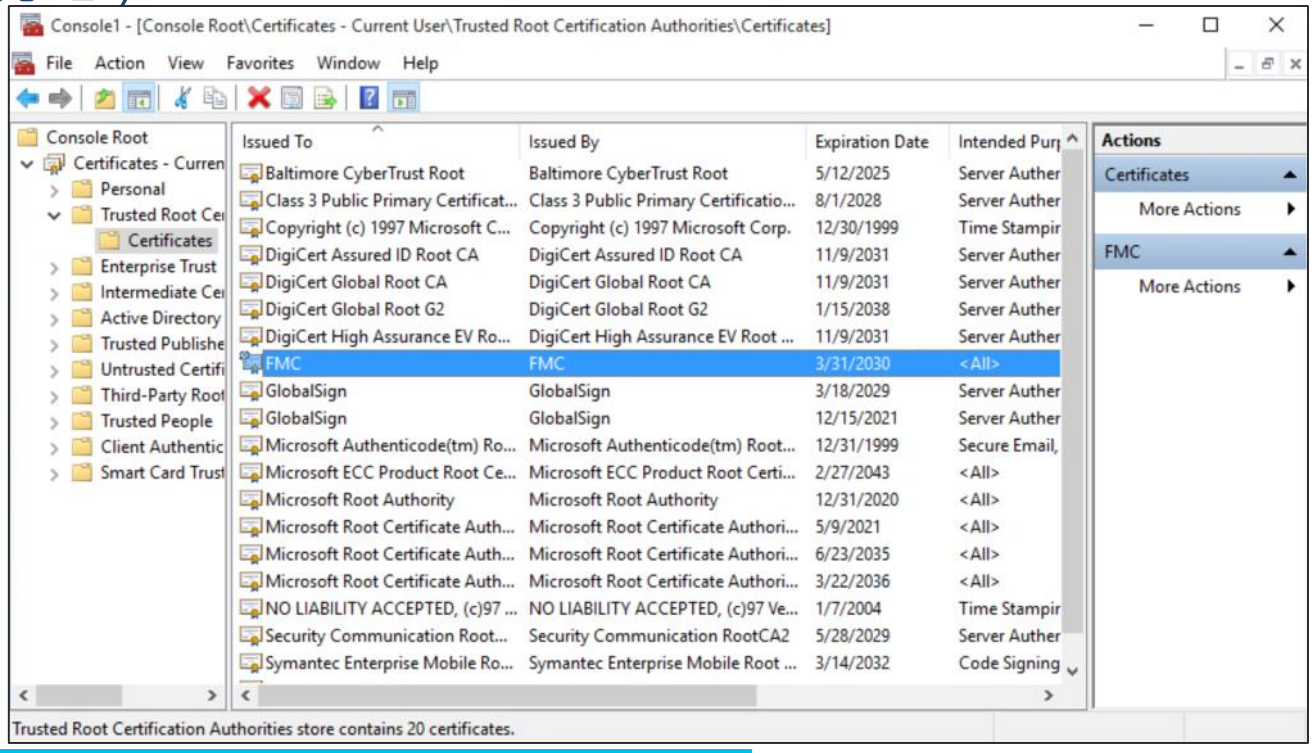






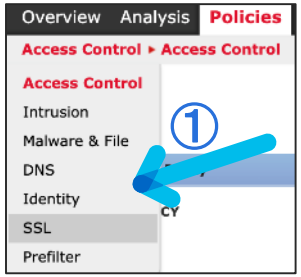
① FMC で設定した PKCS #12 のパスワードを入力し、次へ をクリック
② マニュアルで証明書ストアに「信頼されたルート証明機関」を選択し、次へ をクリック
③ ファイル名や証明書ストアが正しいことを確認し、次へ をクリック

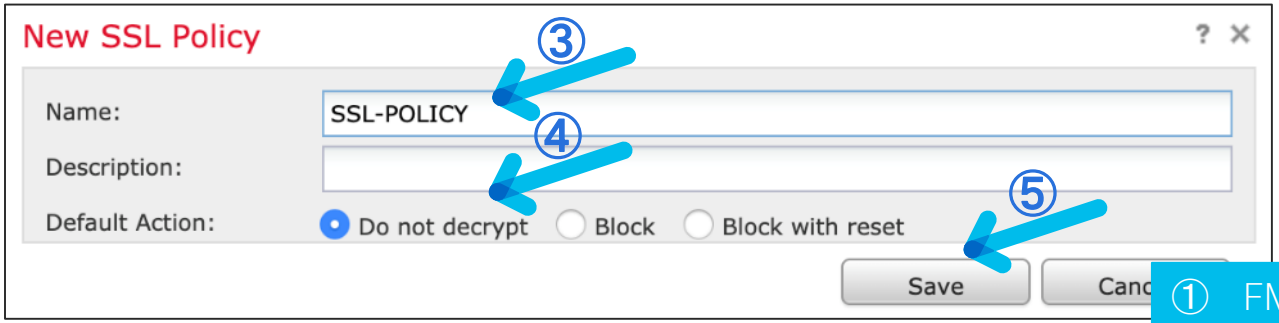
ステップ2-4: PC への Internal CA 証明書のインポート(参考)(続き)



はい をクリックすると Internal CA の証明書がインポートされる
Microsoft 管理コンソール (MMC) からインポートされた証明書が確認可能

ステップ3-1: SSL policy の作成

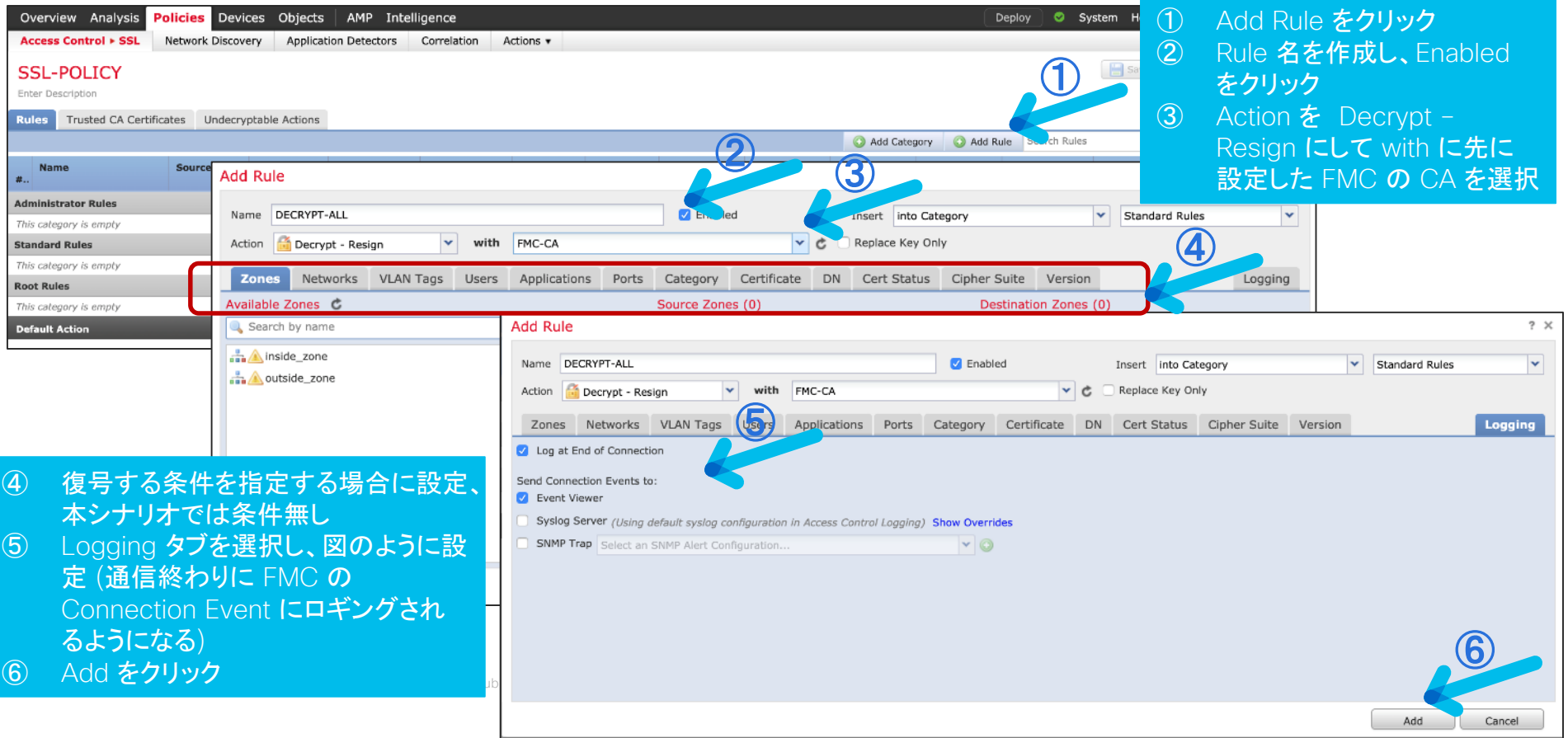




本シナリオでは、簡素化のため、すべての通信において TLS 復号を行うポリシーを適用する。
実際には、FTD の負荷軽減のためにも、条件によっての復号の有無を制定した方が良い。

① FMC にて Policies > SSL を選択
② New Policy をクリック
③ 復号を行うポリシー名を作成
④ Default Action はそのまま (Do not decrypt) で
⑤ Save をクリック

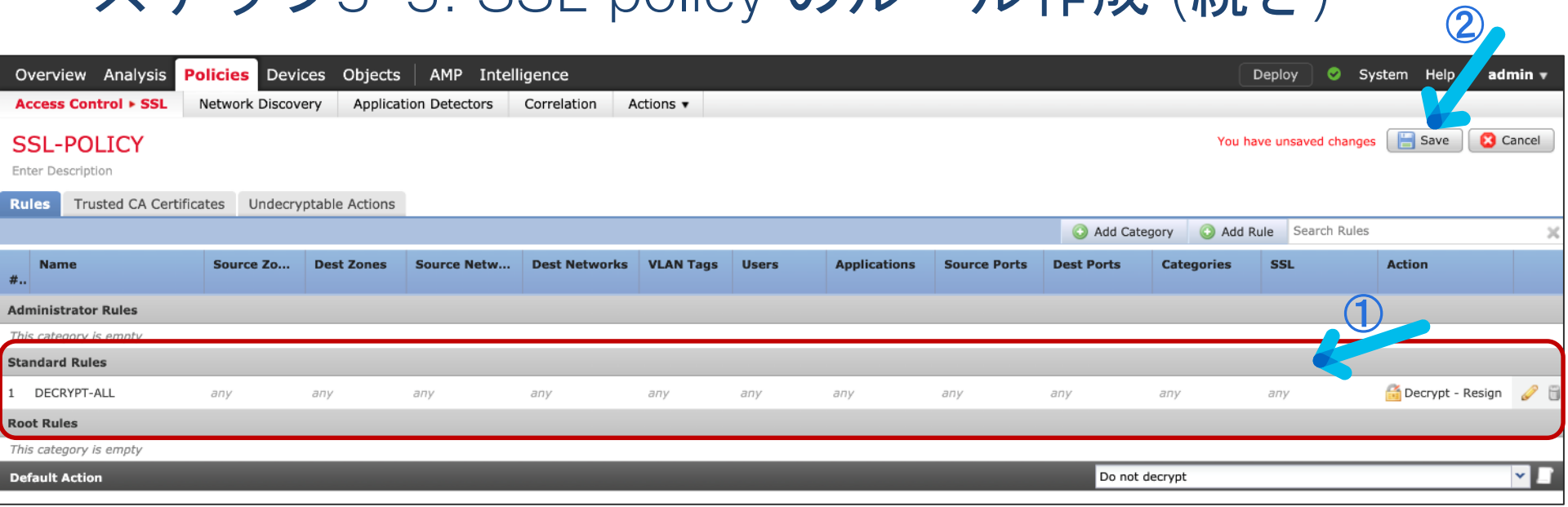
ステップ3-2: SSL policy のルール作成



① Add Rule をクリック
② Rule 名を作成し、Enabled をクリック
③ Action を Decrypt – Resign にして with に先に設定した FMC の CA を選択

④ 復号する条件を指定する場合に設定、本シナリオでは条件無し
⑤ Logging タブを選択し、図のように設定 (通信終わりに FMC の Connection Event にロギングされるようになる)
⑥ Add をクリック

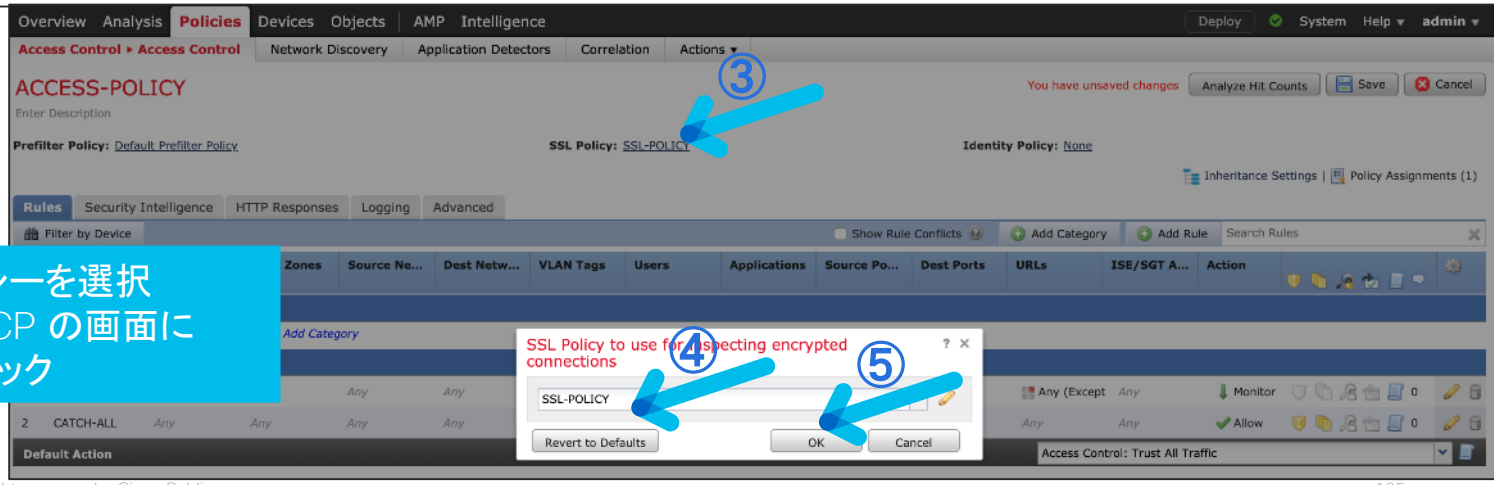
ステップ3-3: SSL policy のルール作成 (続き)



① 設定したルールに間違いがないことを確認
② Save をクリック

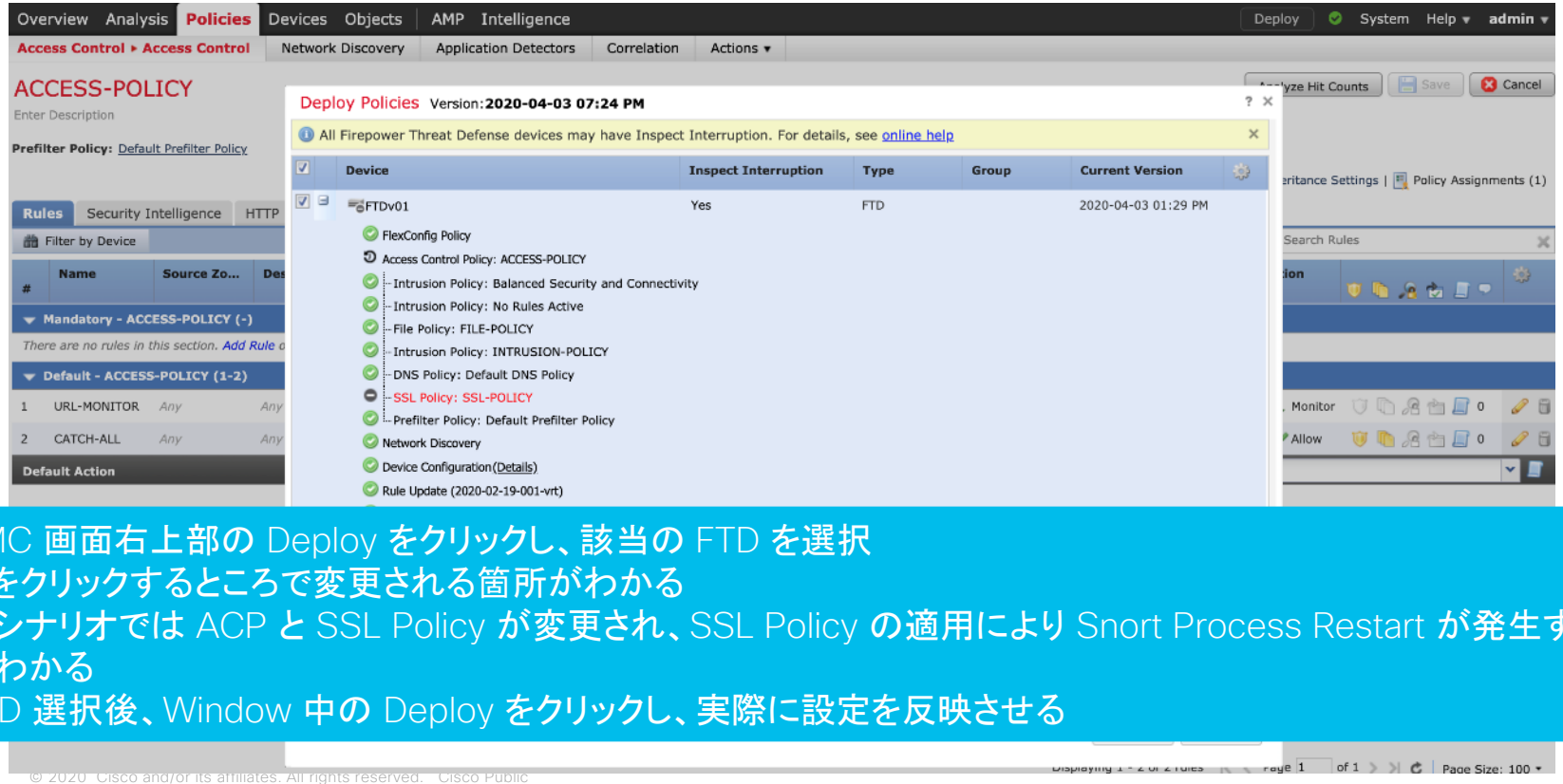
ステップ4-1: Access Control Policy と SSL Policy の紐付け

① Policy > Access Control を選択
② FTD で使っている ACP の鉛筆アイコン (edit) をクリック
③ SSL Policy をクリック



④ 作成した復号ポリシーを選択
⑤ OK をクリックし、ACP の画面に戻って Save をクリック

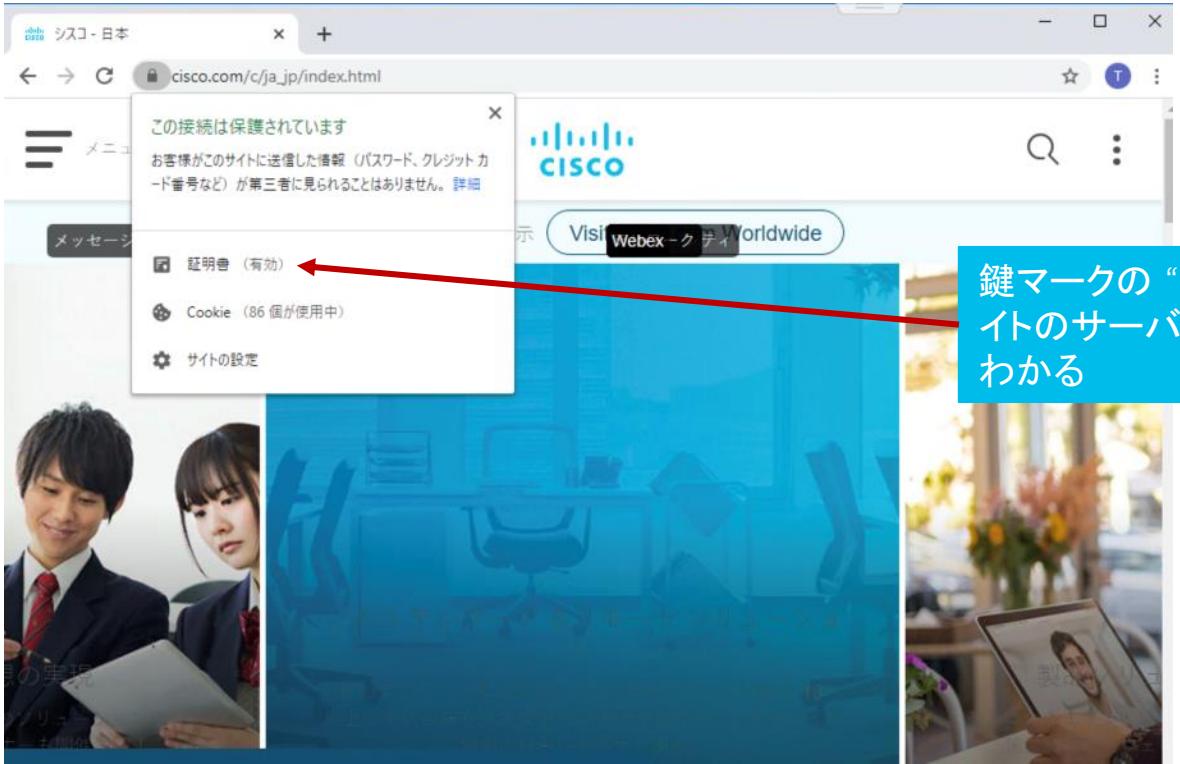
ステップ5-1: 設定の反映



FMC 画面右上部の Deploy をクリックし、該当の FTD を選択
+ をクリックするところで変更される箇所がわかる
本シナリオでは ACP と SSL Policy が変更され、SSL Policy の適用により Snort Process Restart が発生することがわかる
FTD 選択後、Window 中の Deploy をクリックし、実際に設定を反映させる

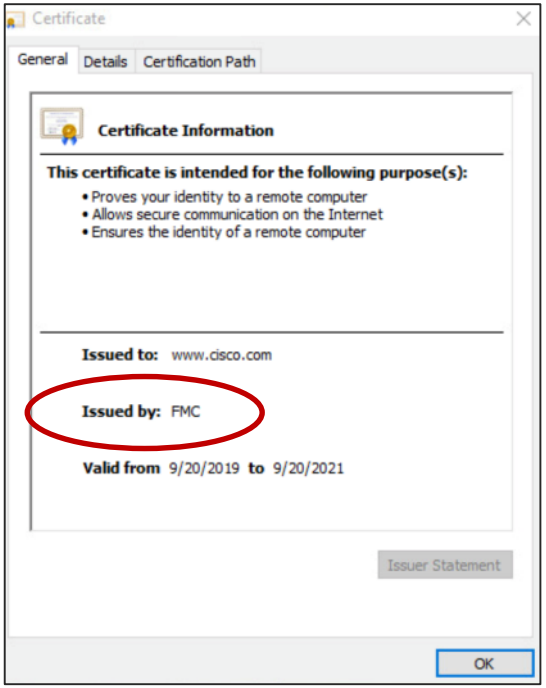
ステップ6-1: PC からの https サイトへの疎通確認

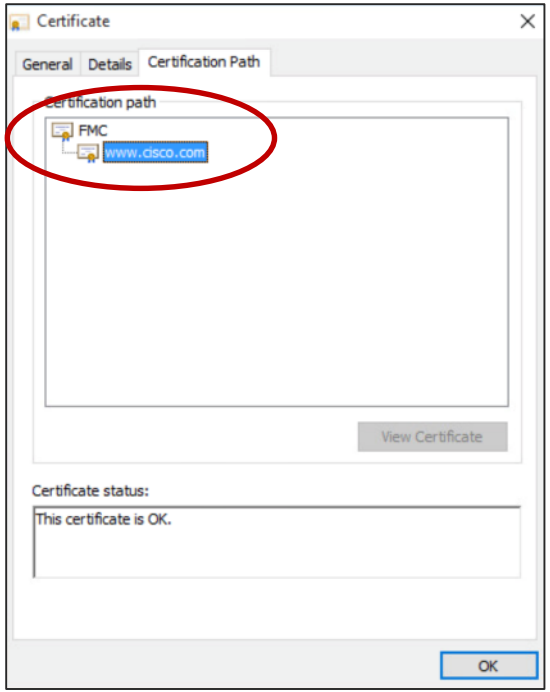
Deploy 終了後、動作確認を行う。テスト PC の Web ブラウザ（今回は Chrome を使用）から任意の https サイトにアクセスし、アドレスバーの鍵マークをクリックすることで、テスト PC として正しい https の通信ができているかどうかが確認できる



鍵マークの “証明書 (有効)” をクリックすると、このサイトのサーバ証明書をどこの CA がサインしたかがわかる

ステップ6-2: PC からの https サイトへの疎通確認(続き)



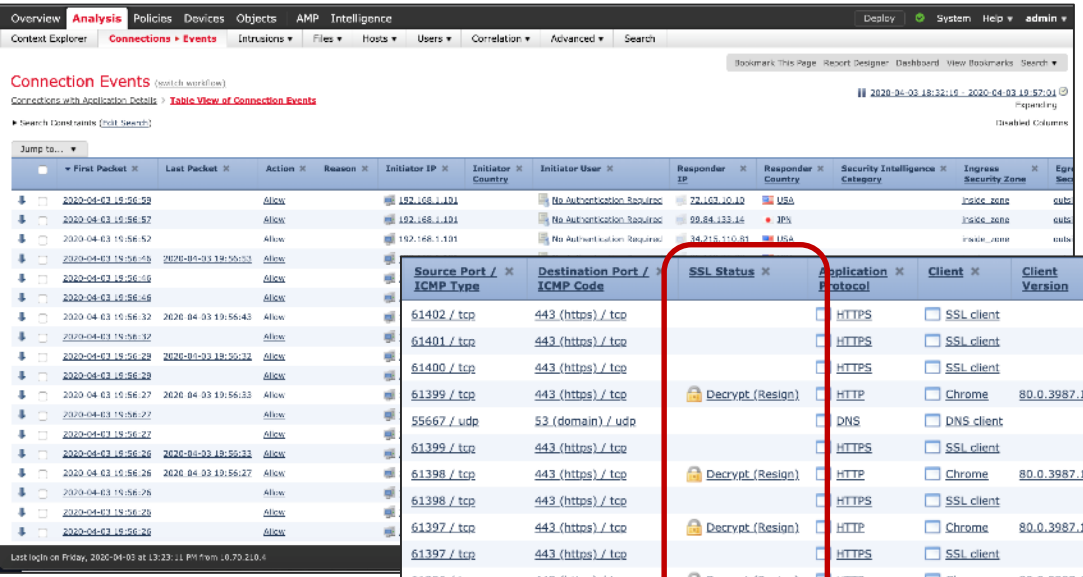


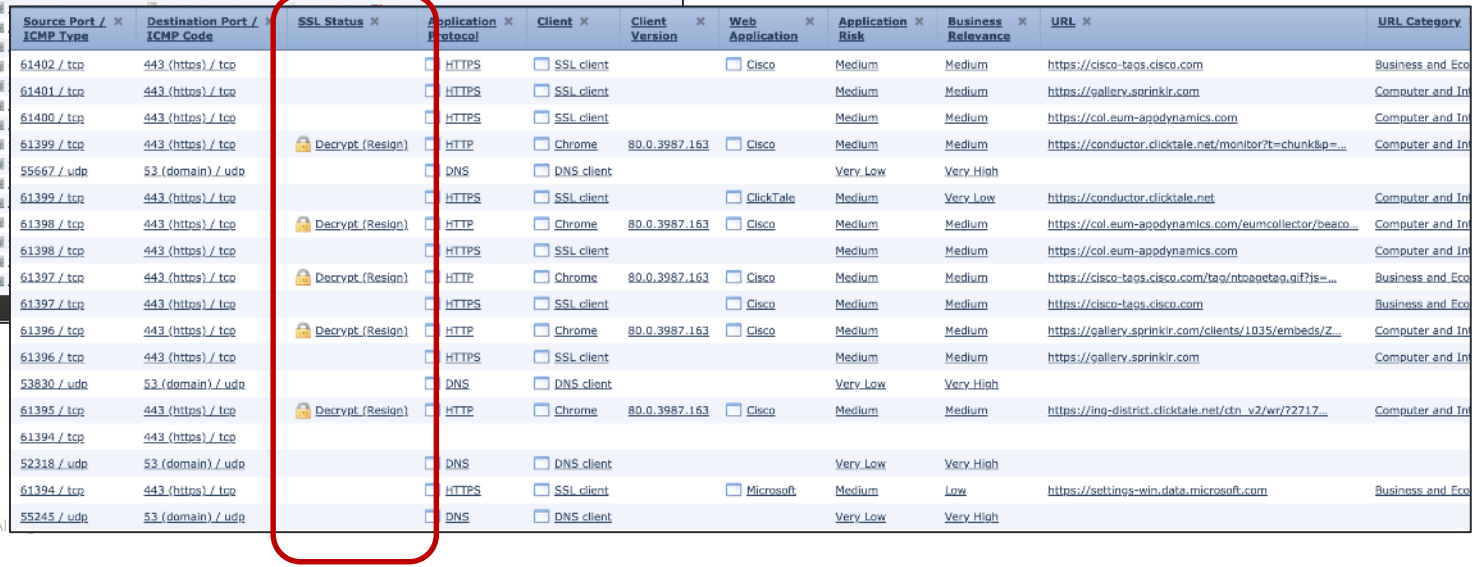
FMC の Internal CA がサインしていることがわかる。
このテスト PC は FMC の Internal CA を信頼しているため、https のエラーにならない

(参考) 実際の www.cisco.com は正規の CA にサインされている

ステップ6-3: PC からの https サイトへの疎通確認

FMC の Connection Event にて、Table View を選択し、右へスクロールする。SSL Status という項目にて、その https の通信が 復号 (outgoing の resign) されていることを確認できる

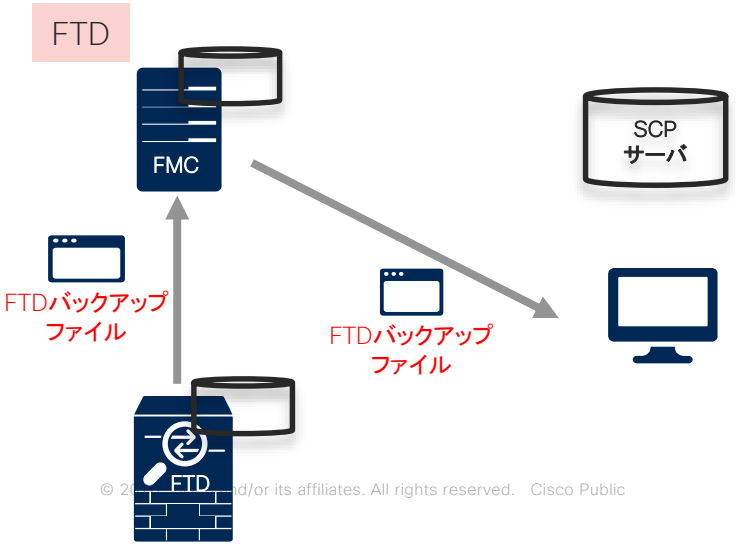


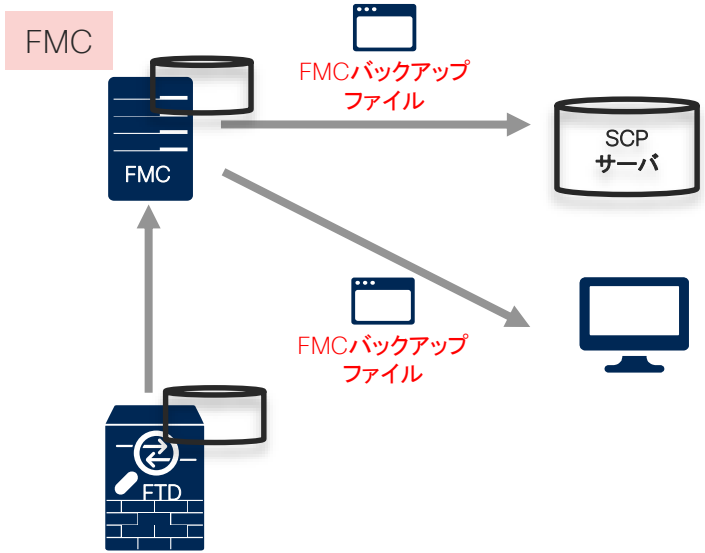


11. バックアップの設定とリストアの方法

バックアップ

- FMC、FTDともにバックアップの取得が可能である。
- FTDバックアップの保存先はFTDローカル、もしくはFMCローカル。
- FMCバックアップはFMCローカルへのダウンロードと並行して、リモートサーバ(SCP)へコピーも可能。
- FMCに保存したバックアップファイルは、FMCのGUIより端末へダウンロードすることができる。





操作の流れ

- ステップ1 :FTDデバイスのバックアップ取得
- ステップ2 :FTDデバイスのバックアップファイル確認
- ステップ3 :FMCのバックアップ取得
- ステップ4 :FMCのバックアップファイル確認

- SCPサーバが、FMCより疎通の取れるネットワークセグメントに構築してある前提とする

※FTD,FMCともにHA化してあってもバックアップ取得は可能

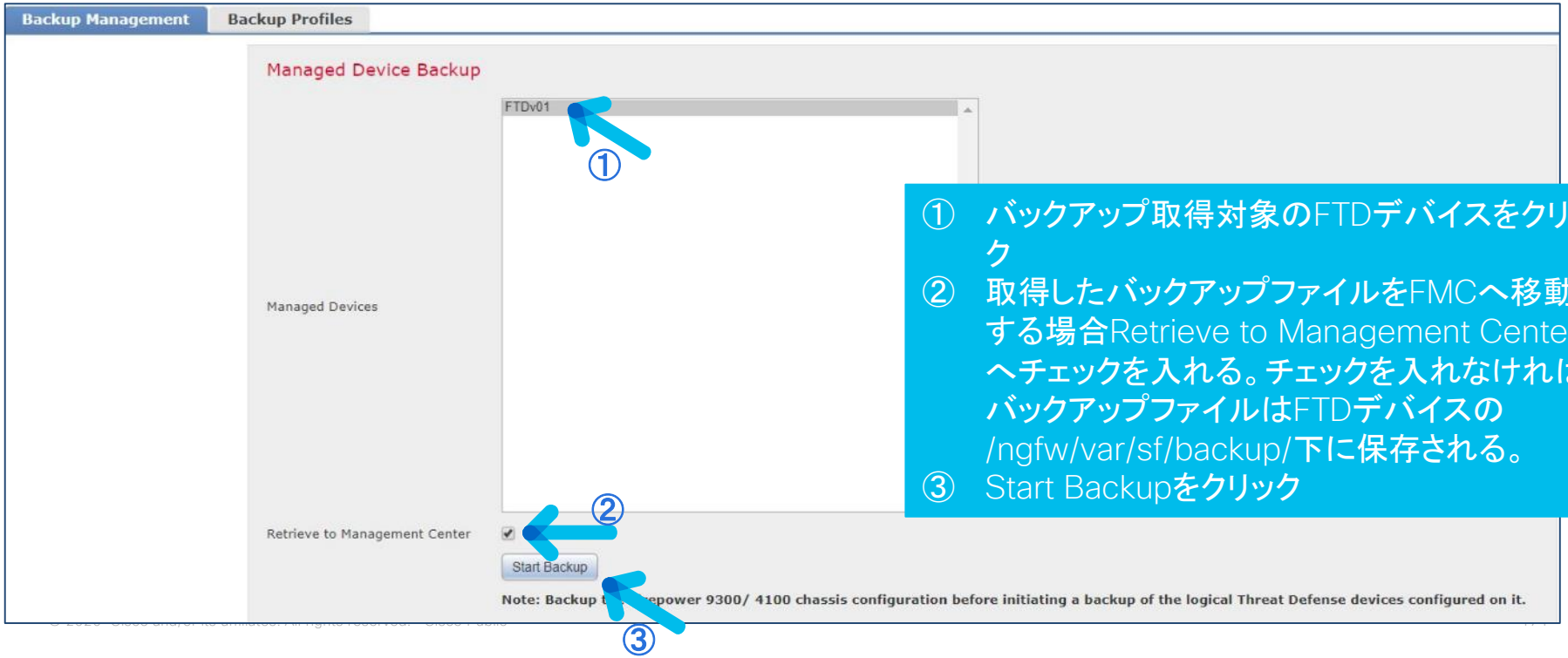
ステップ 1: FTDデバイスのバックアップ取得①

- FMCの管理下にあるFTDデバイスのバックアップを取得する。

① Systemを選択
② Tools下のBackup/Restoreを選択
③ Managed Device Backupをクリック

ステップ 1: FTDデバイスのバックアップ取得②

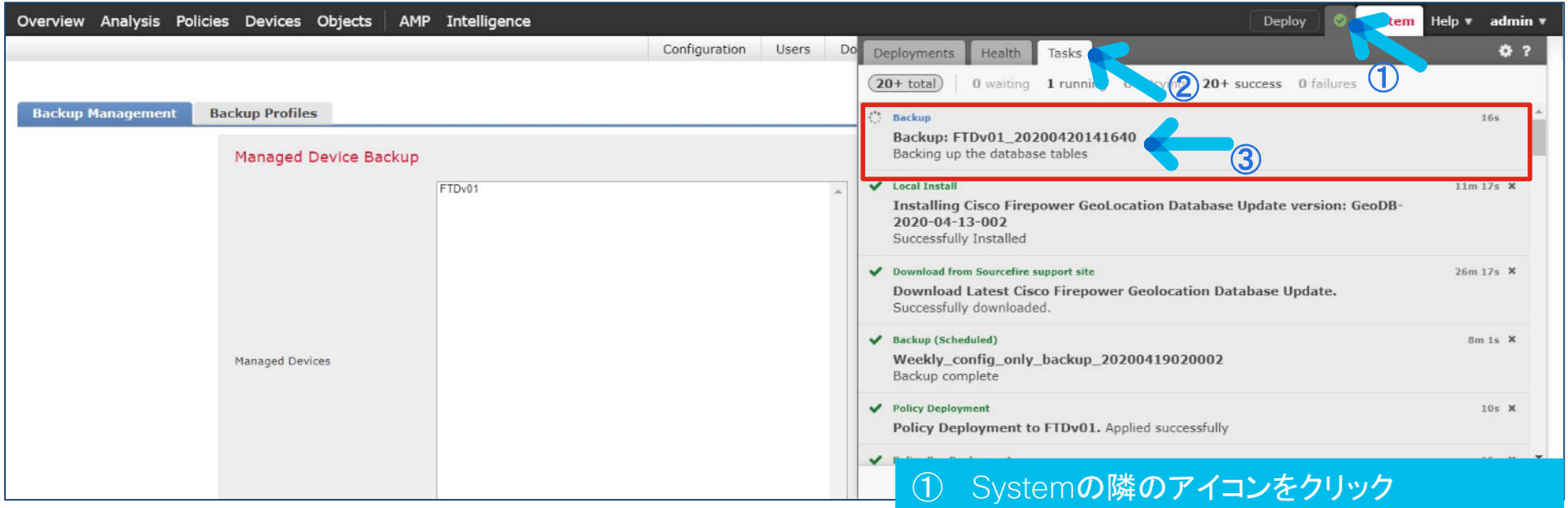
- バックアップの取得対象とするFTDデバイスを指定する。



① バックアップ取得対象のFTDデバイスをクリック
② 取得したバックアップファイルをFMCへ移動する場合Retrieve to Management Centerへチェックを入れる。チェックを入れなければバックアップファイルはFTDデバイスの/ngfw/var/sf/backup/下に保存される。
③ Start Backupをクリック

ステップ 1: FTDデバイスのバックアップ取得③

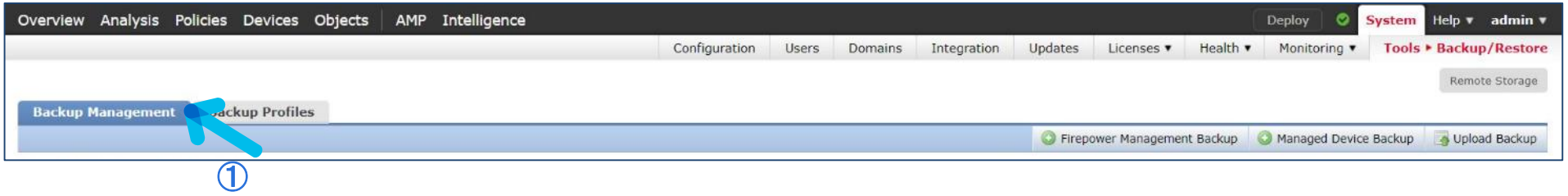
- バックアップ処理の進行状況を確認する。

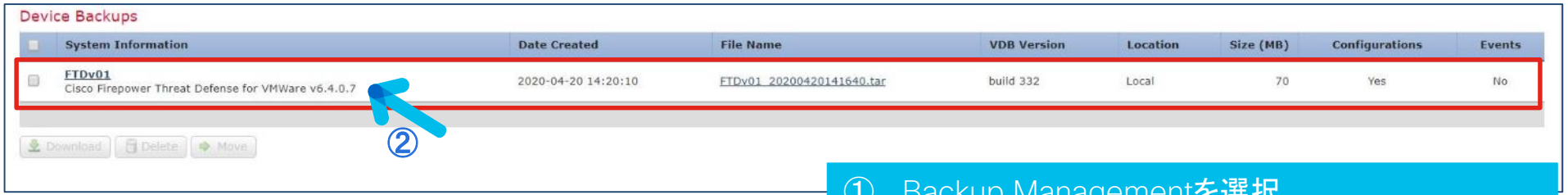


① Systemの隣のアイコンをクリック
② Tasksを選択
③ “Backup”という項目名でタスクが進行していることを確認できる。

ステップ 2: FTDデバイスのバックアップ取得確認

- バックアップ処理の完了後、取得したバックアップファイルを確認する。





① Backup Managementを選択
② Device Backups下に、FTDデバイスのバックアップファイルが表示されていることを確認

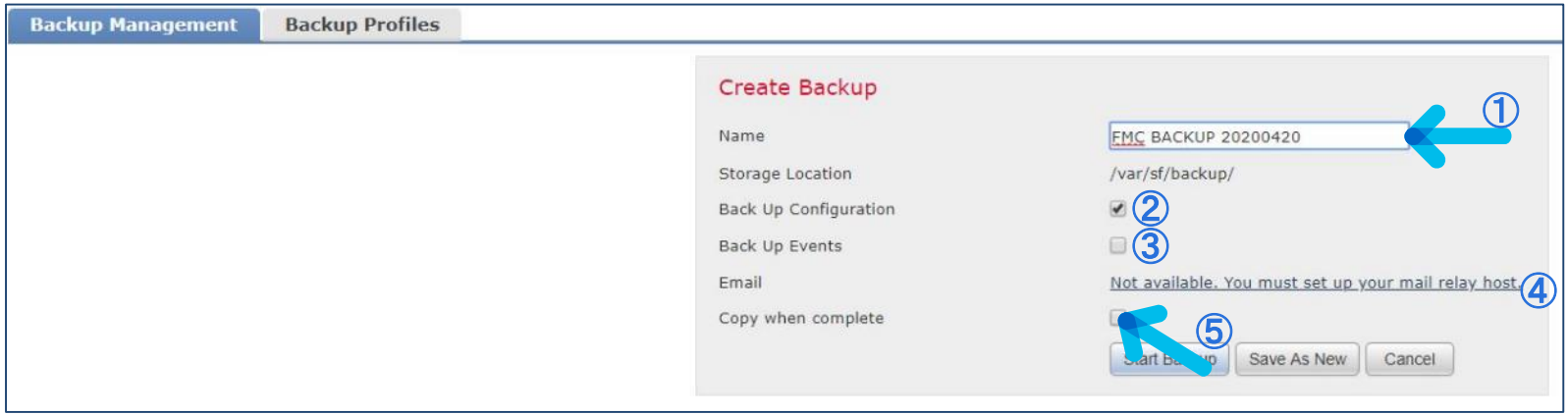
ステップ 3: FMCのバックアップ取得①

- FMC自身のバックアップを取得する。

① Systemを選択
② Tools下のBackup/Restoreを選択
③ Firepower Management Backupをクリック

ステップ 3: FMCのバックアップ取得②

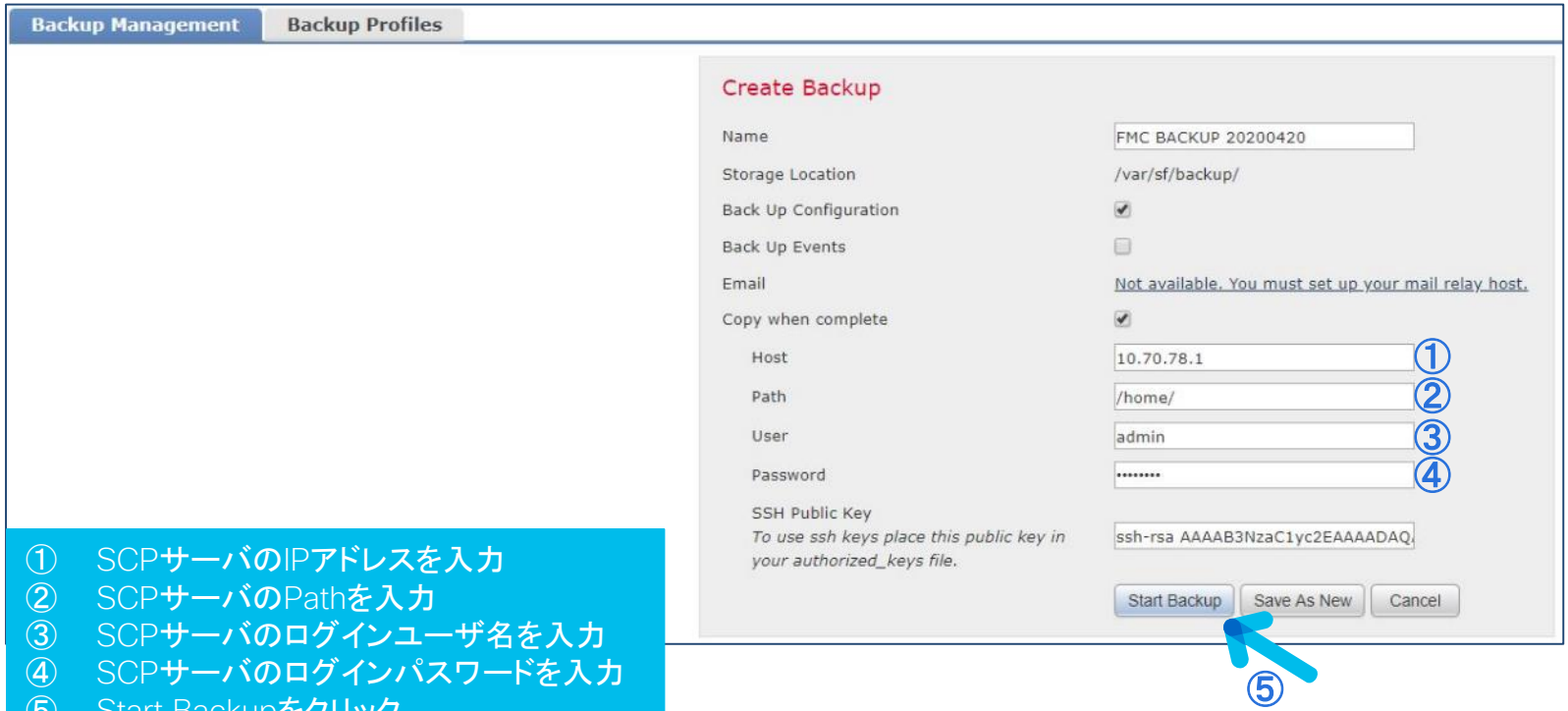
- バックアップ取得における各項目を指定する。



① バックアップ名を入力。ここでは”FMC BACKUP 20200420”とする
② Configurationのバックアップを含める場合チェックを入れる
③ イベントログのバックアップを含める場合チェックを入れる
④ バックアップ取得後にメール通知を行う場合設定する
⑤ バックアップ完了後にSCPサーバへバックアップファイルをコピーする場合にチェックを入れる

ステップ 3: FMCのバックアップ取得③

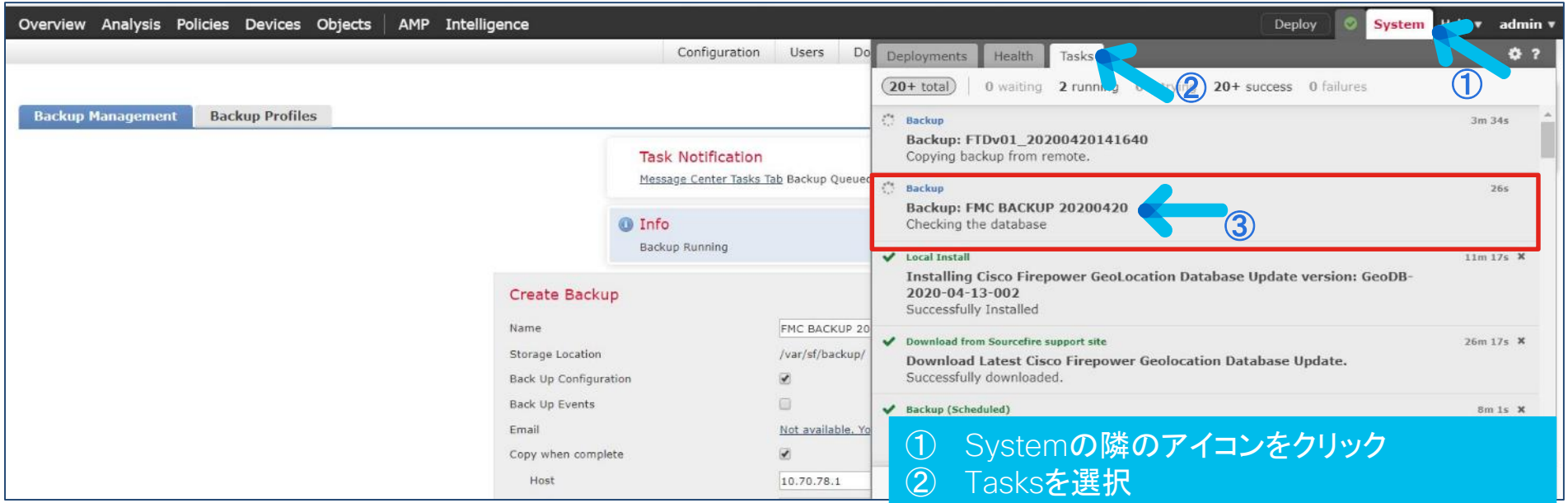
- バックアップファイルをSCPサーバへコピーする場合の、各項目を指定する。



① SCPサーバのIPアドレスを入力
② SCPサーバのPathを入力
③ SCPサーバのログインユーザ名を入力
④ SCPサーバのログインパスワードを入力
⑤ Start Backupをクリック

ステップ 3: FMCのバックアップ取得④

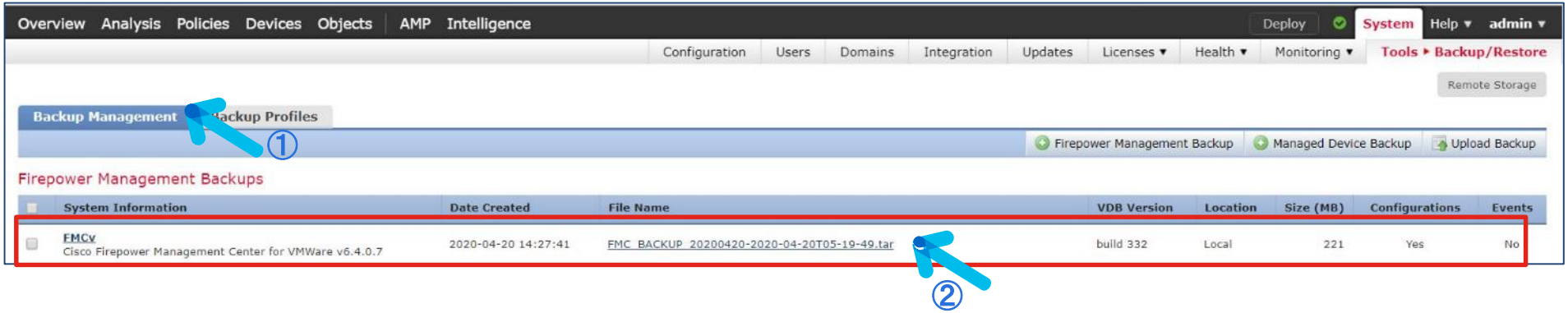
- バックアップ処理の進行状況を確認する。



① Systemの隣のアイコンをクリック
② Tasksを選択
③ “Backup”という項目名の下で” FMC BACKUP 20200420”の名前でタスクが進行していることを確認できる。

ステップ 4: FMCのバックアップ取得確認

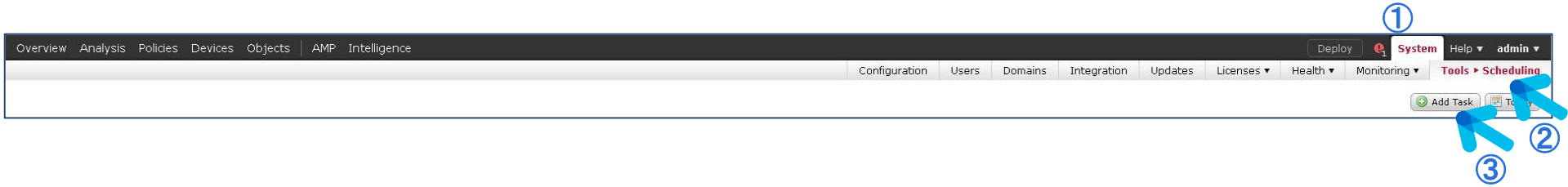
- バックアップ処理の完了後、取得したバックアップファイルを確認する。



① Backup Managementを選択
② Firepower Management Backups下に、FMCのバックアップファイルが表示されていることを確認

参考:スケジュール バックアップ生成①

- スケジュールタスクにて、バックアップ生成タスクを定義する。



① Systemを選択
② Tools下のSchedulingを選択
③ Add Taskをクリック

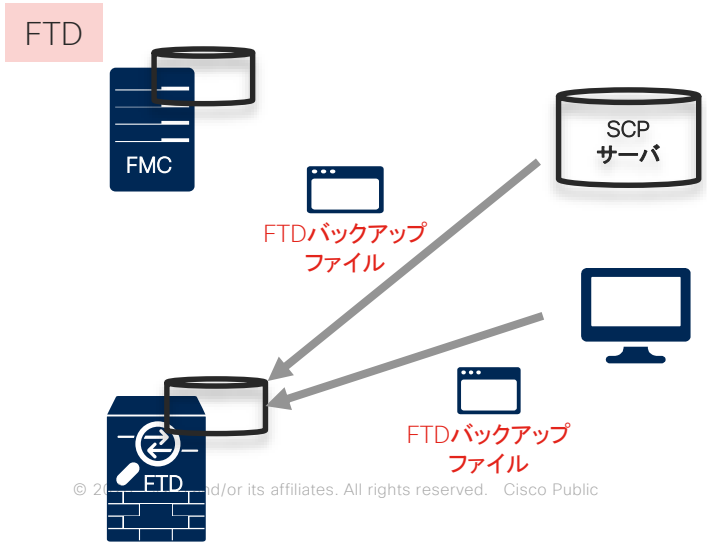
参考:スケジュール バックアップ生成②

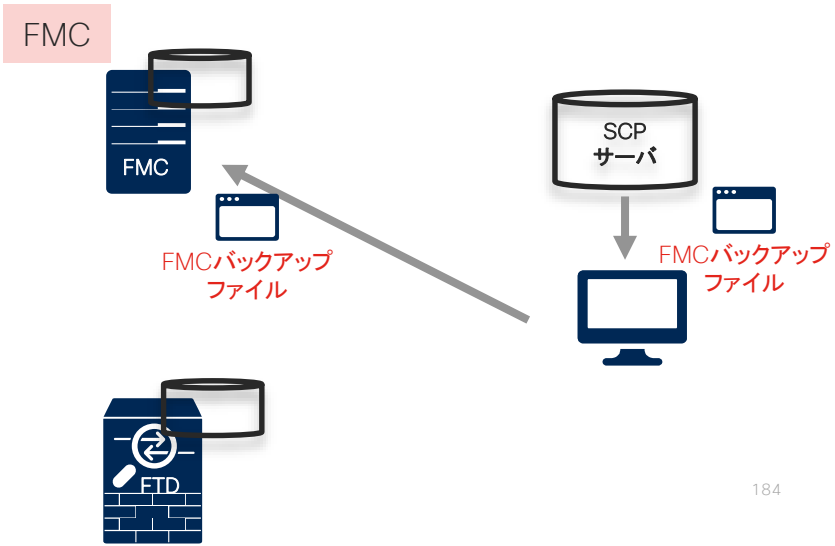
- スケジュールタスクにて、バックアップ生成タスクを定義する。

① プルダウンよりBackupをを選択
② Recurringへチェックを入れる
③ レポート生成タスクの開始年月日を指定。ここでは2020年4月11日とする。
④ バックアップ生成タスクの頻度を指定。ここでは週次とし、毎週日曜日の午前4:00に処理を開始する設定をしている
⑤ Job Nameを入力。ここでは”SCHEDULE BACKUP”とする
⑥ Backup Typeにてバックアップ取得する対象をFMC、FTDデバイスより指定する。
⑦ Backup Profileを指定する。
⑧ Saveをクリック

リストア

- FMC、FTDともにバックアップより設定のリストアが可能である。
- FTDリストアは、取得済みのバックアップをSCPサーバ、もしくはFTDローカルへアップロードして実施する。
- FMCリストアは、取得済みのバックアップファイルをFMCローカルへアップロードして実施する。





操作の流れ

- ステップ1：FMCバックアップファイルのアップロード
- ステップ2：FMCのリストア
- ステップ3：FTDデバイスのリストア

- SCPサーバが、FMCより疎通の取れるネットワークセグメントに構築してある前提とする

ステップ 1: FMCバックアップファイルのアップロード①

- 機器交換の場合など、リストアに使用するバックアップファイルがFMCローカルに存在しない場合、取得済みのFMCバックアップファイルを、FMCローカルへアップロードする。

① Systemを選択
② Tools下のBackup/Restoreを選択
③ Upload Backupをクリック

- 機器交換の場合、交換機はバックアップ取得機器とソフトウェア、パッチ、VDB、SRUバージョンを同一とすること

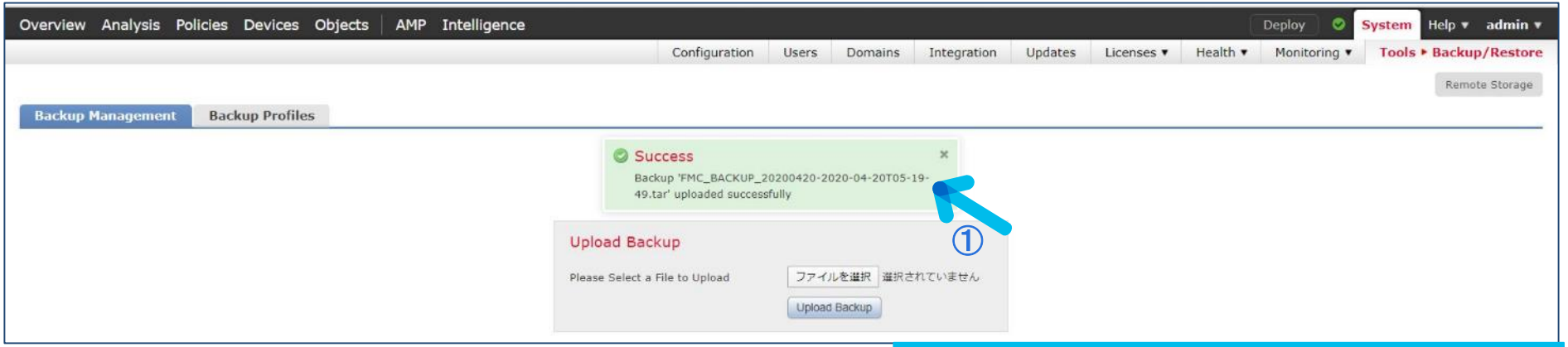
ステップ 1: FMCバックアップファイルのアップロード②

- 取得済みのFMCバックアップファイルを、FMCローカルへアップロードする。

① アップロードするFMCバックアップファイルを指定
② Upload Backupをクリック

ステップ 1: FMCバックアップファイルのアップロード③

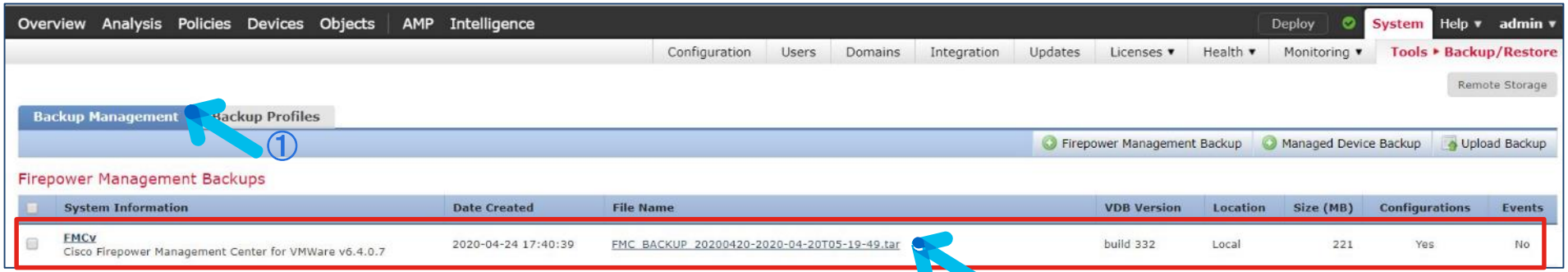
- バックアップファイルのアップロードが終了したことの確認。



① アップロードの終了メッセージを確認

ステップ 1: FMCバックアップファイルのアップロード④

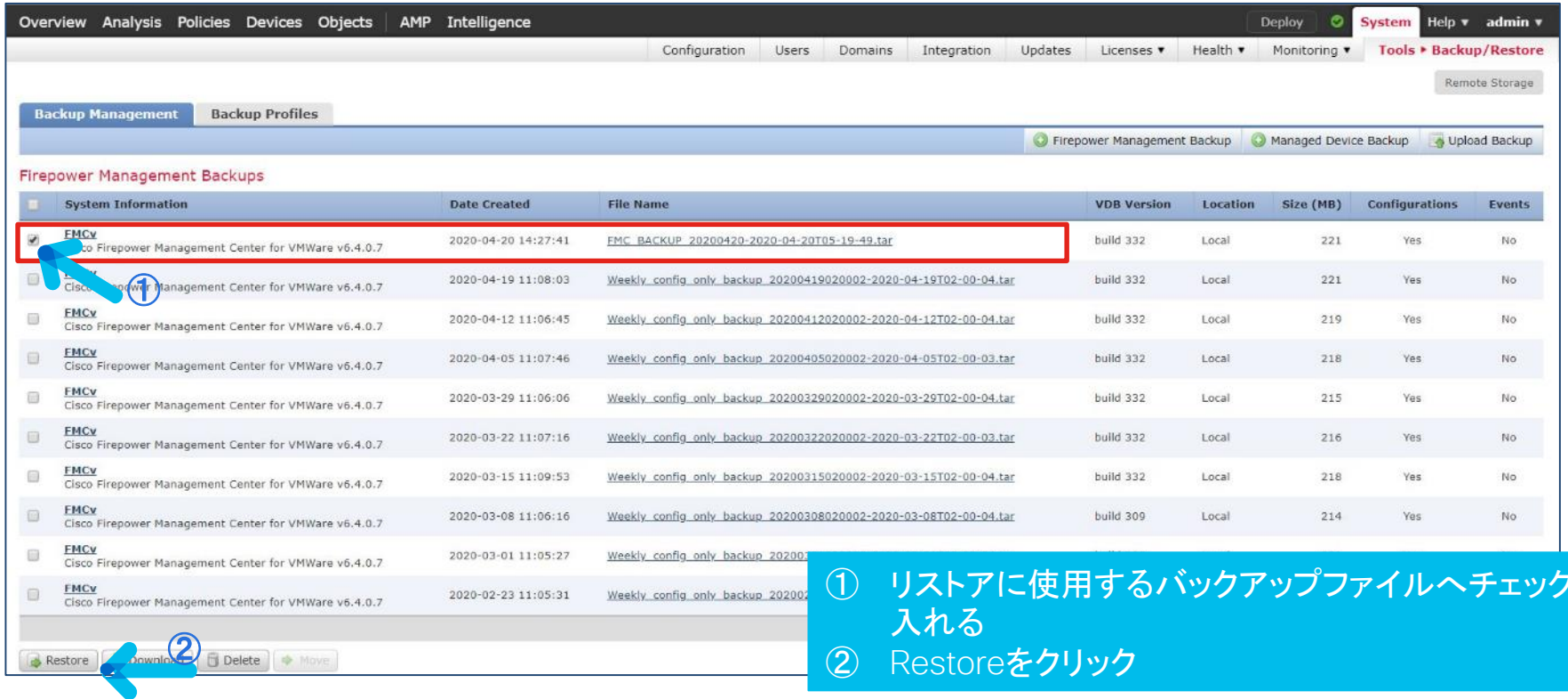
- アップロード処理が完了すると、Backup ManagementのFirepower Management Backups下にも、バックアップファイルが表示される。



① Backup Managementを選択
② Firepower Management Backups下に、アップロードしたFMCのバックアップファイルが表示されていることを確認

ステップ 2: FMCのリストア①

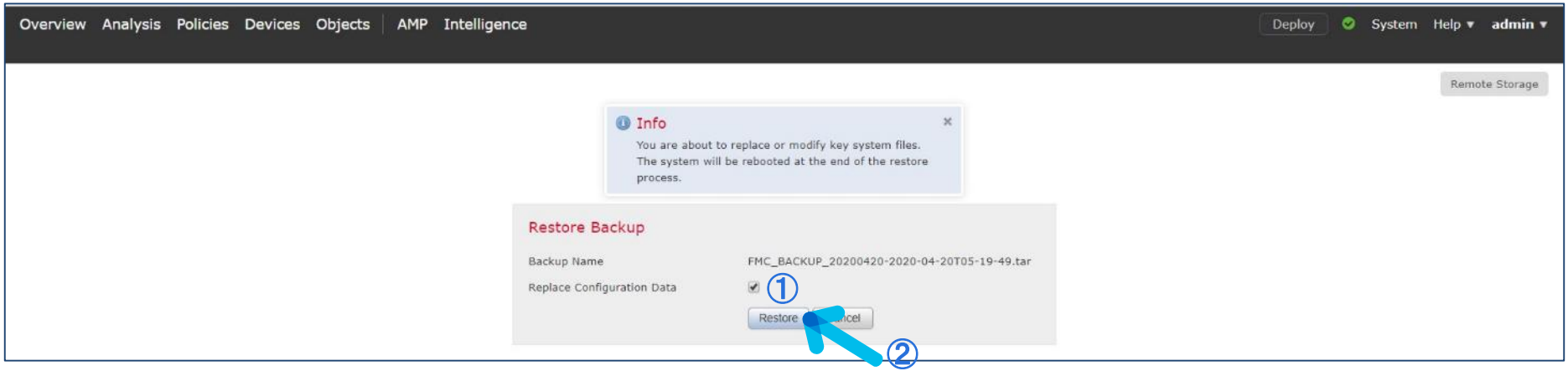
- リストアに使用する、バックアップファイルの選択。



① リストアに使用するバックアップファイルへチェックを入れる
② Restoreをクリック

ステップ 2: FMCのリストア②

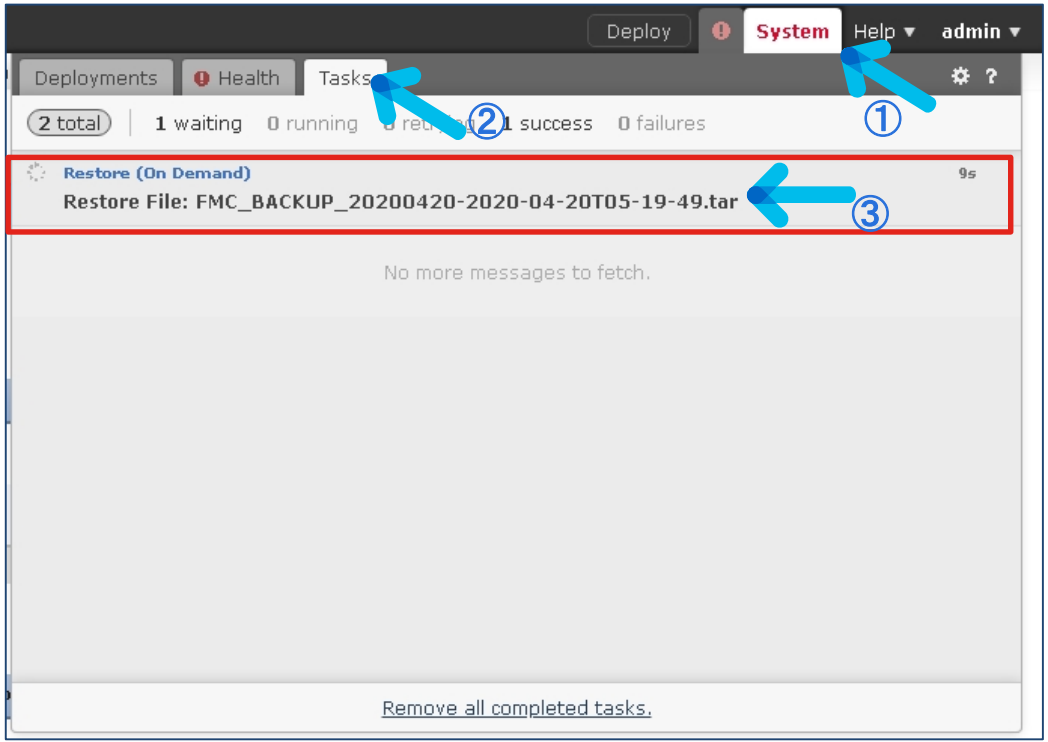
- リストアに使用する、バックアップファイルの選択。



① リストアファイルのConfigurationで設定を上書きする場合チェックを入れる
② Restoreをクリック

ステップ 2: FMCのリストア③

- リストア処理の開始を確認する。

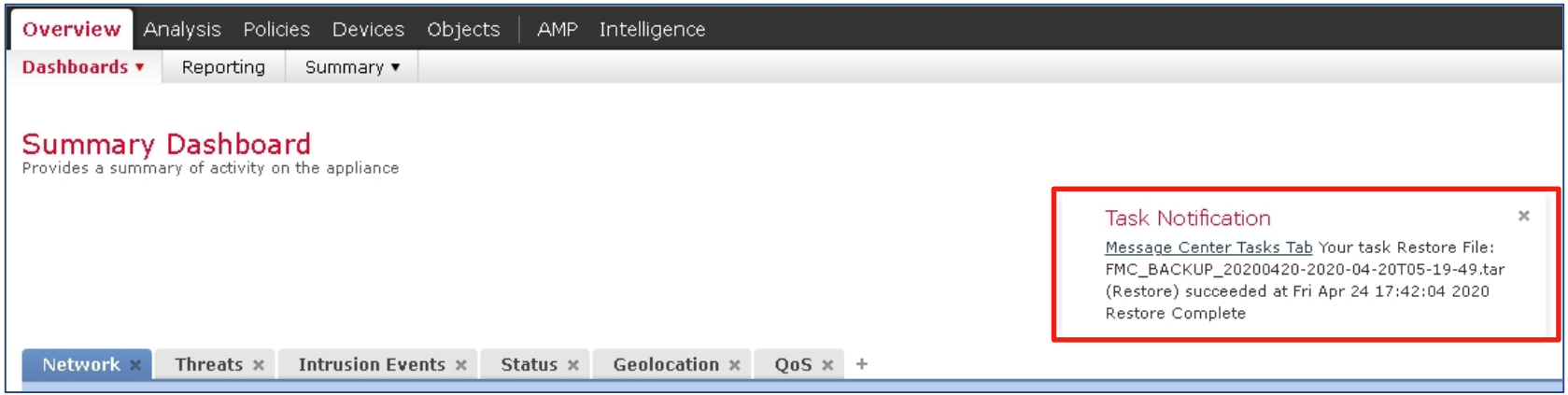


① Systemの隣のアイコンをクリック
② Tasksを選択
③ “Restore”という項目名の下で”Restore File”の名前でタスクが進行していることを確認できる。

- リストア完了後に機器が再起動

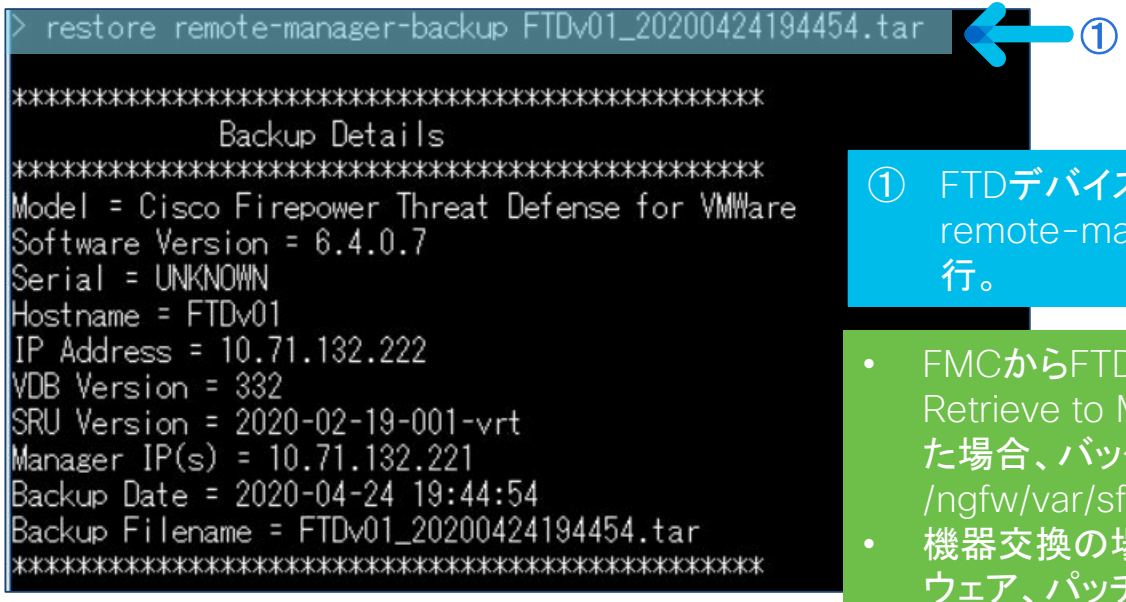
ステップ 2: FMCのリストア④

- 再起動後のFMCへログインした際の表示。



ステップ 3: FTDデバイスリストア ローカルバックアップファイル使用①

- FTDローカルのバックアップファイルを利用してリストアを実行する場合。



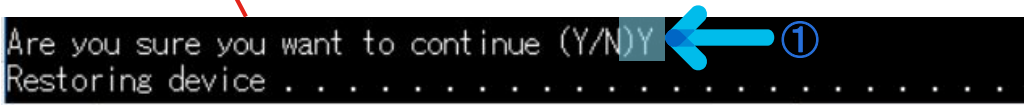
① FTDデバイスへCLI、SSHでログインして”restore remote-manager-backup *[バックアップファイル名]*”を実行。

- FMCからFTDデバイスバックアップを取得する際に、Retrieve to Management Centerへチェックを入れなかった場合、バックアップファイルはFTDデバイスの/ngfw/var/sf/backup/へ保存されている
- 機器交換の場合、交換機はバックアップ取得機器とソフトウェア、パッチ、VDB、SRUバージョンを同一とすること
- FMC上では、リストア対象のFTDデバイス情報は削除しないこと。FTDはリストア後にFMCに自動接続するため、にFMC側で登録を残しておく必要がある。

ステップ 3: FTDデバイスリストア ローカルバックアップファイル使用②

- Backup Detailの内容に問題のないことを確認して、リストア処理を実行。

```
Backup Date = 2020-04-24 19:44:54
Backup Filename = FTDv01_20200424194454.tar
**************************************************



********************* Caution *****************************
Verify that you are restoring a valid backup file. Make sure that software, SRU and VDB Versions on this device match versions from the backup manifest before proceeding.
Restore operation will overwrite all configurations on this device with the configurations in backup. Kindly ensure the old device is disconnected from the network to avoid IP conflict.
**********************************************************

Are you sure you want to continue (Y/N)Y
Restoring device . . . . . .
```



① “Y”を入力

- リストア完了後に機器が再起動

ステップ 3: FTDデバイスリストア リモートバックアップファイル使用①

- 事前にSCPサーバへバックアップファイルをアップロードし、このバックアップファイルを利用してリストアを実行する場合。

```
> restore remote-manager-backup location 10.70.78.1 admin /home/ FTDv01_20200420141640.tar
Enter SCP password:

***********************************************
            Backup Details
***********************************************
Model = Cisco Firepower Threat Defense for VMWare
Software Version = 6.4.0.7
Serial = UNKNOWN
Hostname = FTDv01
IP Address = 10.71.132.222
VDB Version = 332
SRU Version = 2020-02-19-001-vrt
Manager IP(s) = 10.71.132.221
Backup Date = 2020-04-20 14:16:40
Backup Filename = FTDv01_20200420141640.tar
***********************************************
```

① FTDデバイスへCLI、SSHでログインして”restore remote-manager-backup location *[SCPサーバホスト名/IPアドレス] [SCPサーバ ログインユーザ] [バックアップファイル フォルダ] [バックアップファイル名]*”を実行。

- 機器交換の場合、交換機はバックアップ取得機器とソフトウェア、パッチ、VDB、SRUバージョンを同一とすること
- FMC上では、リストア対象のFTDデバイス情報は削除しないこと。FTDはリストア後にFMCに自動接続するため、にFMC側で登録を残しておく必要がある。

ステップ 3: FTDデバイスリストア リモートバックアップファイル使用②

- Backup Detailの内容に問題のないことを確認して、リストア処理を実行。

```
Backup Date = 2020-04-20 14:16:40
Backup Filename = FTDv01_20200420141640.tar
************************************************



********************* Caution ****************************
Verify that you are restoring a valid backup file. Make sure that software, SRU and VDB Versions on this device match versions from the backup manifest before proceeding.
Restore operation will overwrite all configurations on this device with the configurations in backup. Kindly ensure the old device is disconnected from the network to avoid IP conflict.
************************************************************

Are you sure you want to continue (Y/N)Y
Restoring device . . . . . .
```

① “Y”を入力

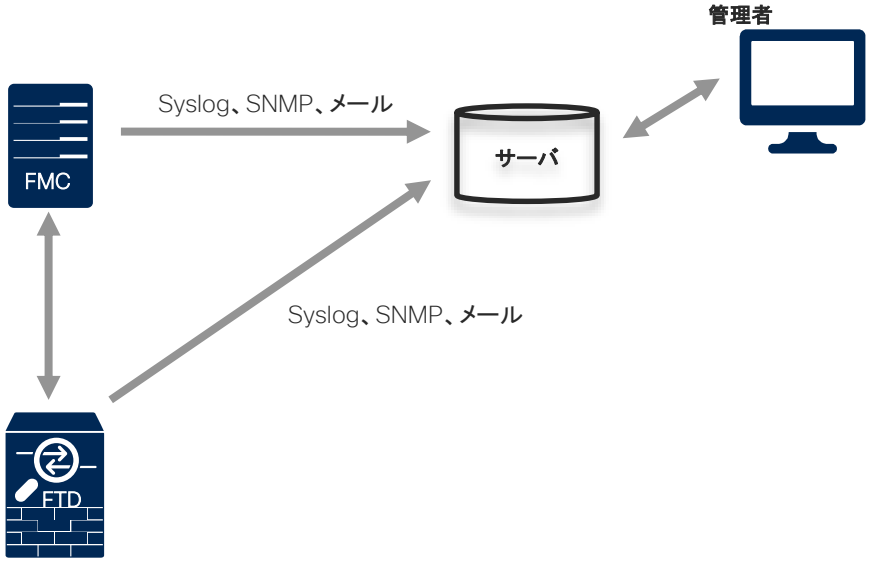
- リストア完了後に機器が再起動

12. Syslog・レポート・アラートの設定

Syslogサーバへのロギング

ロギング概要

- 各種アラート、イベントはFMC内部へ保存し、FMC GUIで表示するほかに、外部サーバへ通知を送ることができる。
- 本資料では特にSyslogサーバへのロギングについて記載する。



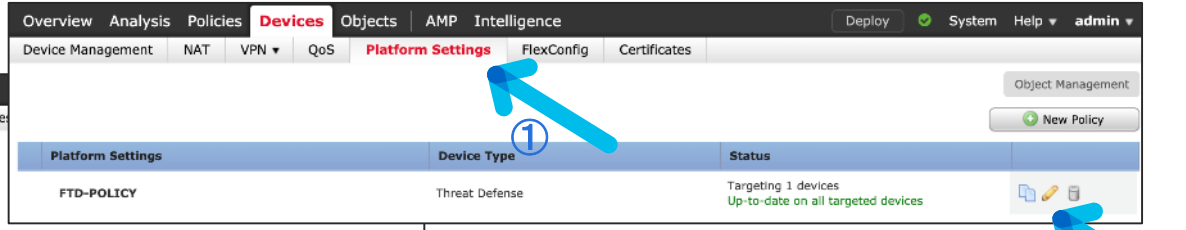
設定の流れ

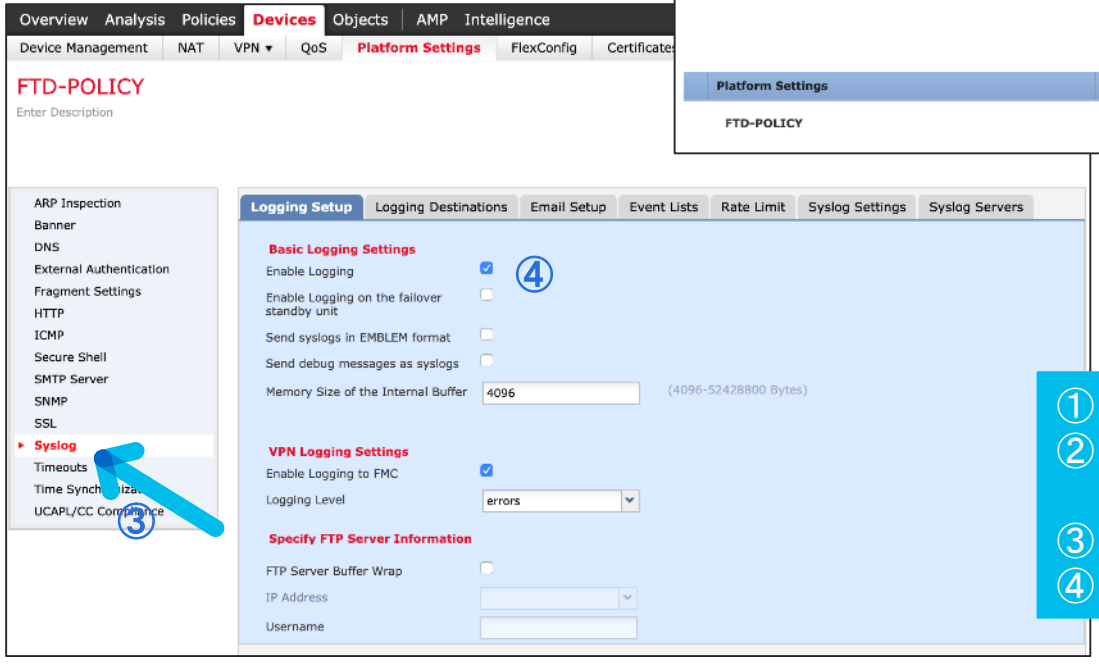
- ステップ1 : Logging Setup設定
- ステップ2 : Logging Destination設定
- ステップ3 : Syslog Settings設定
- ステップ4 : Syslog Servers設定

- Syslogサーバが、FMCより疎通の取れるネットワークセグメントに構築してある前提とする

ステップ 1: Logging Setup設定

- ロギングの設定を行う



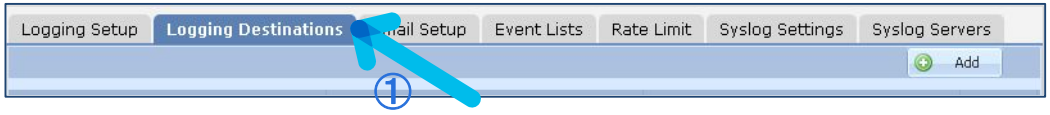


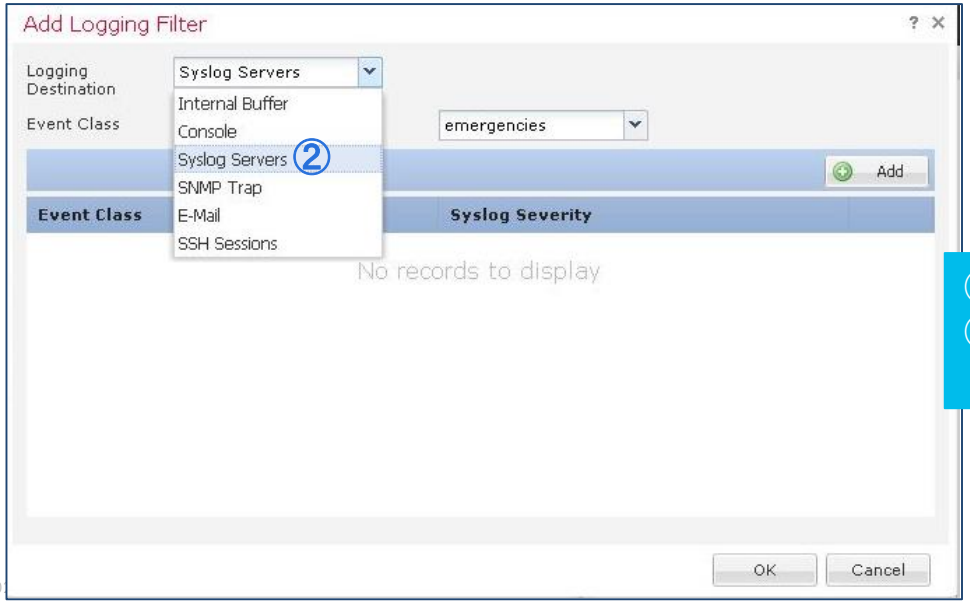
① Device > Platform Settingsをクリック
② 2章で作成済みのFTD-POLICYの鉛筆マークをクリック
③ Syslogを選択
④ Enable Loggingにチェックを入れる

- 左側メニューでSMTP Server、SNMPをクリックすることでメール、SNMP設定が可能

ステップ 2: Logging Destination設定①

- ログの送付先を指定する

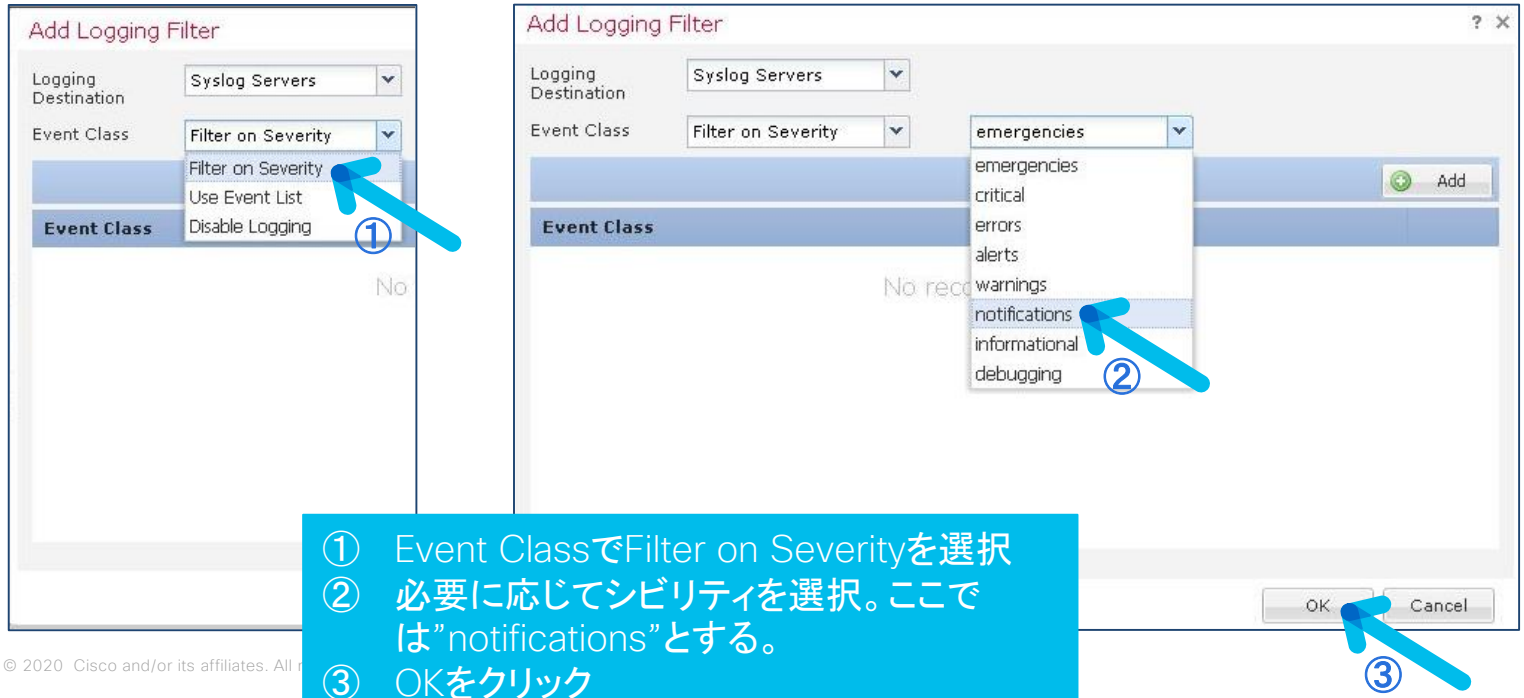




① Logging Destinationを選択
② Logging DestinationでSyslog Serversを選択

ステップ 2: Logging Destination設定②

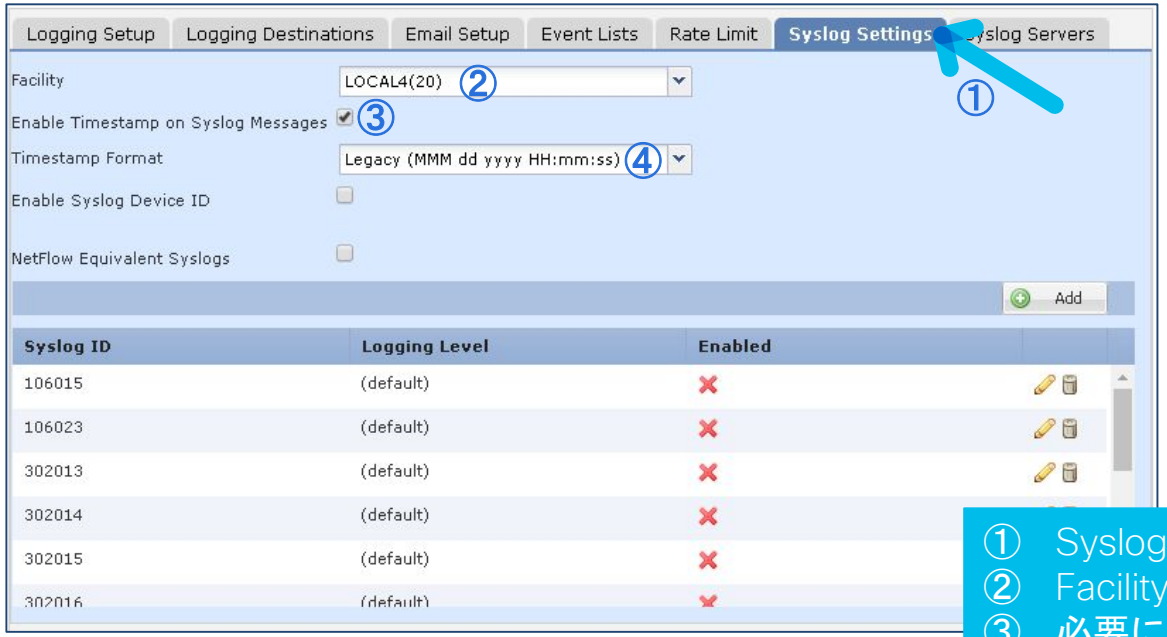
- 送付するログの種別を指定する



① Event ClassでFilter on Severityを選択
② 必要に応じてシビリティを選択。ここでは”notifications”とする。
③ OKをクリック

ステップ 3:Syslog Settings設定

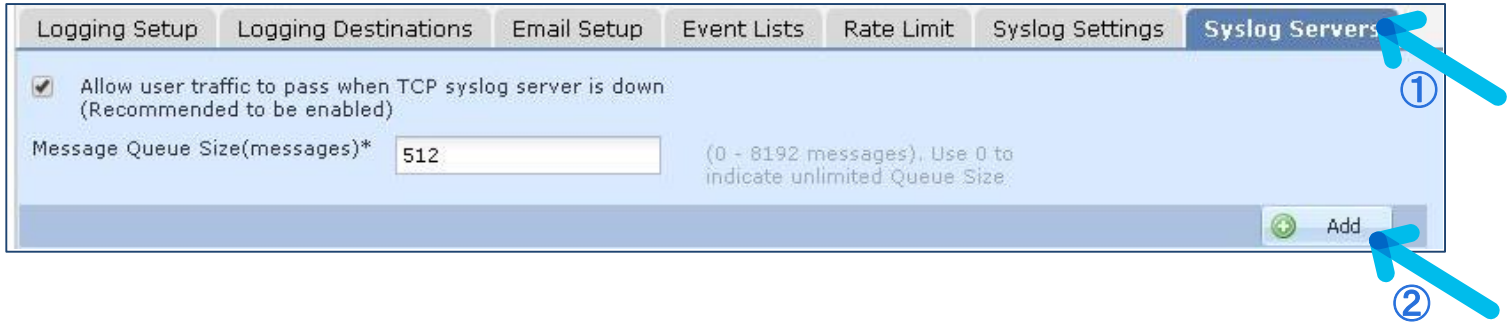
- Syslogメッセージの出力設定を行う



① Syslog Settingsを選択
② Facilityを選択
③ 必要に応じてEnable Timestamp on Syslog Messagesにチェックを入れる
④ Timestamp Formatを選択

ステップ 4:Syslog Servers設定①

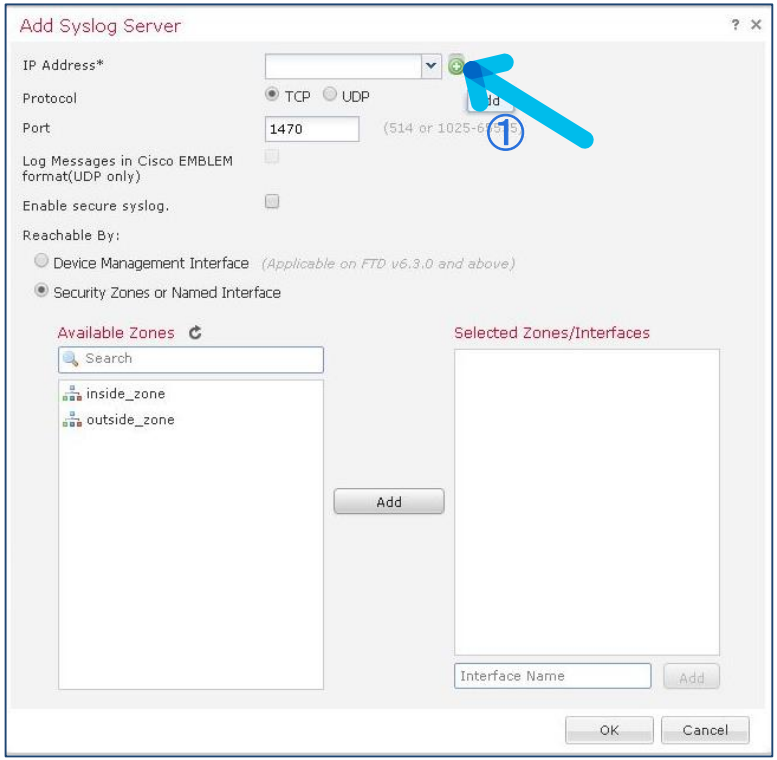
- Syslogメッセージを出力する先のSyslogサーバ設定を行う

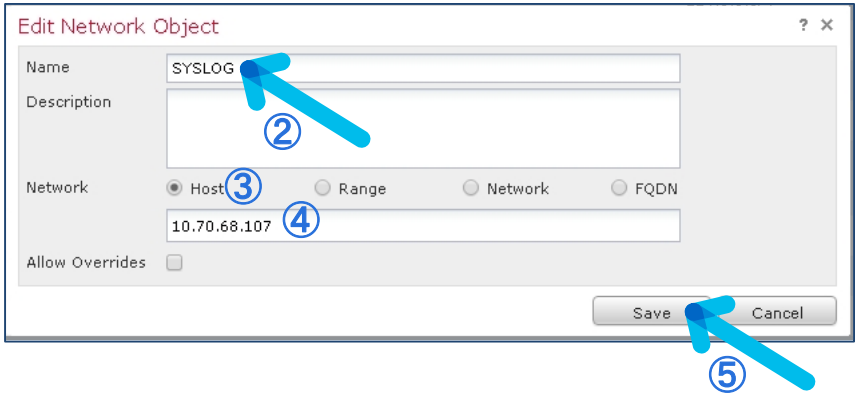


① Syslog Serversを選択
② Addをクリック

ステップ 4:Syslog Servers設定②

- Syslogメッセージを出力する先のSyslogサーバ設定を行う

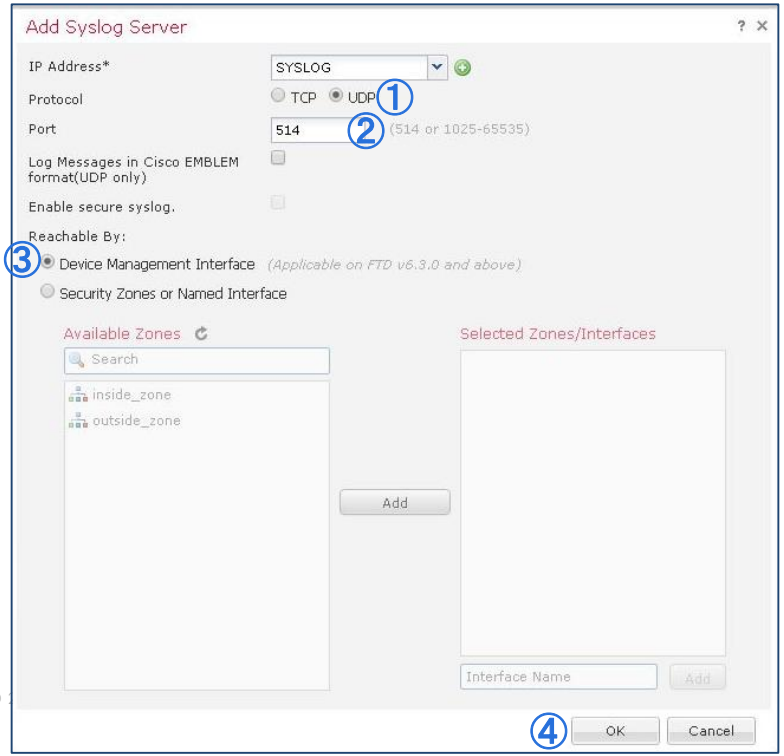




① 緑の追加アイコンをクリック。Network Object作成画面が開く
② Nameを入力。ここでは”SYSLOG”とする
③ Network種別のHostにチェックを入れる
④ SyslogサーバのIPアドレスを入力
⑤ Saveをクリック

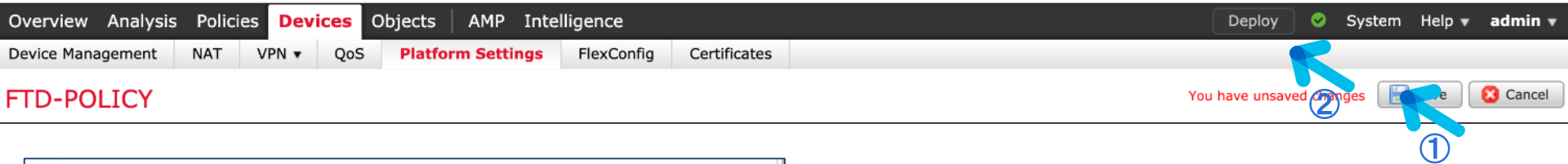
ステップ 4:Syslog Servers設定③

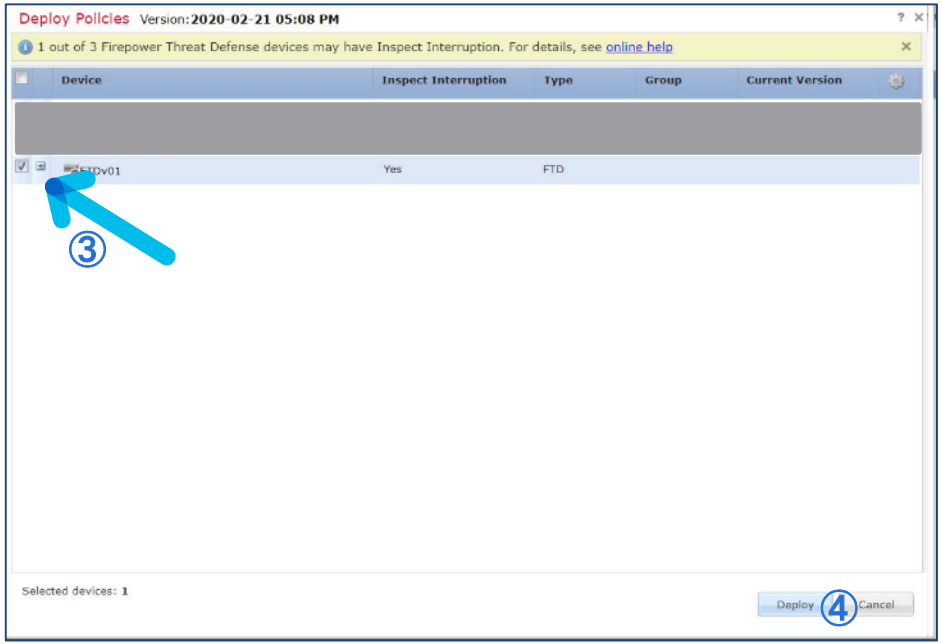
- Syslogメッセージを出力する先のSyslogサーバ設定を行う



① Syslogメッセージ送信プロトコルを選択する。ここではUDPを選択する
② 同様にポートを指定する。ここでは514とする。
③ Reachable ByでSyslogメッセージの送信元とするインターフェイスを選択する。ここでは”Device Management Interface”とする
④ OKをクリック

ステップ 5: Deploy





① Saveをクリック
② Deployをクリック
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をクリック

参考: Syslogメッセージの出力例

- 例えばFTDのインターフェイスGigaEthernet0/0、0/1のDownとUpを行った場合、Syslogサーバへは下記のようにメッセージが出力される。

```
Apr  8 08:10:26 FTDv01 %FTD-4-411002: Line protocol on Interface GigabitEthernet0/0, changed state to down
Apr  8 08:10:26 FTDv01 %FTD-4-411002: Line protocol on Interface GigabitEthernet0/1, changed state to down
Apr  8 08:12:06 FTDv01 %FTD-4-411001: Line protocol on Interface GigabitEthernet0/0, changed state to up
Apr  8 08:12:06 FTDv01 %FTD-4-411001: Line protocol on Interface GigabitEthernet0/1, changed state to up
```

アラート

アラート概要

- FMC、FTDが生成するアラートは外部サーバへロギングすることが可能。
- 対象となるアラートは下記となる。

項目	説明
Health Monitor Event	機器自体のステータスに関するアラート。
Audit Log Event	監査ログのアラート。
Connection Event	Access Control Policyによるコネクションイベントのアラート。
Discovery Event	Network Discoveryのアラート。
Impact Alert	Intrusion Policy イベントのうち、Impact Flagに応じたアラート。
Intrusion Event	Intrusion Policyのアラート。
Correlation Event	Correlation Policyのアラート。詳細な条件を指定し、アラート通知を実行。
Network Malware Event	Network AMPのアラート。

設定の流れ

- ステップ1：Health Policy確認
- ステップ2：Syslog Alert作成
- ステップ3：Health Alert作成とSyslog Alert関連付け

- Syslogサーバが、FMCより疎通の取れるネットワークセグメントに構築してある前提とする

ステップ 1: Health Policy確認①

- デフォルトで定義されているHealth Policyを確認

① Systemを選択
② Health下のPolicyを選択
③ デフォルトで定義されているHealth Policy横の鉛筆アイコンをクリック

- デフォルト定義のHealth PolicyはDescription欄に” Initial Health Policy”と記載がある。

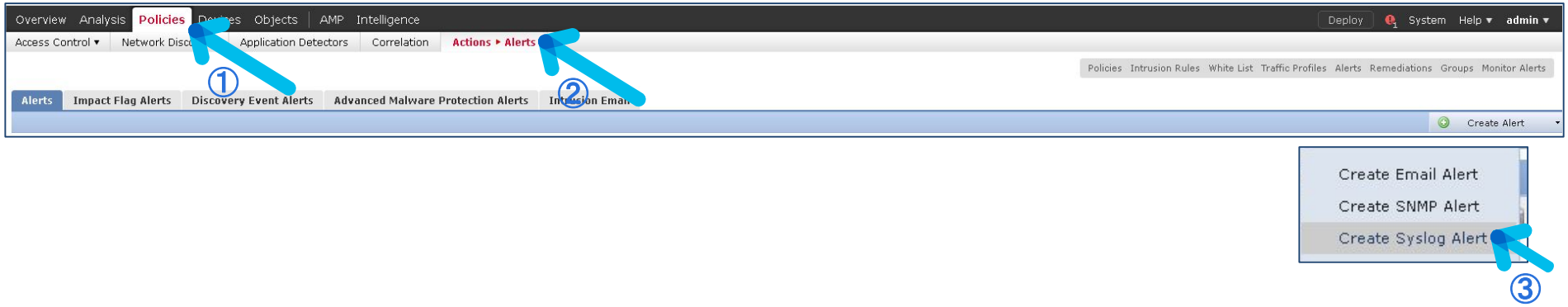
ステップ 1: Health Policy確認②

- デフォルトで定義されているHealth Policyを確認

- 各種アラートの設定を確認する。
- 例えばAMP for Endpoints StatusのEnabledのOnにチェックが入っているため、このアラートは有効であるとわかる。

ステップ 2: Syslog Alert作成①

- Syslog Alertを作成

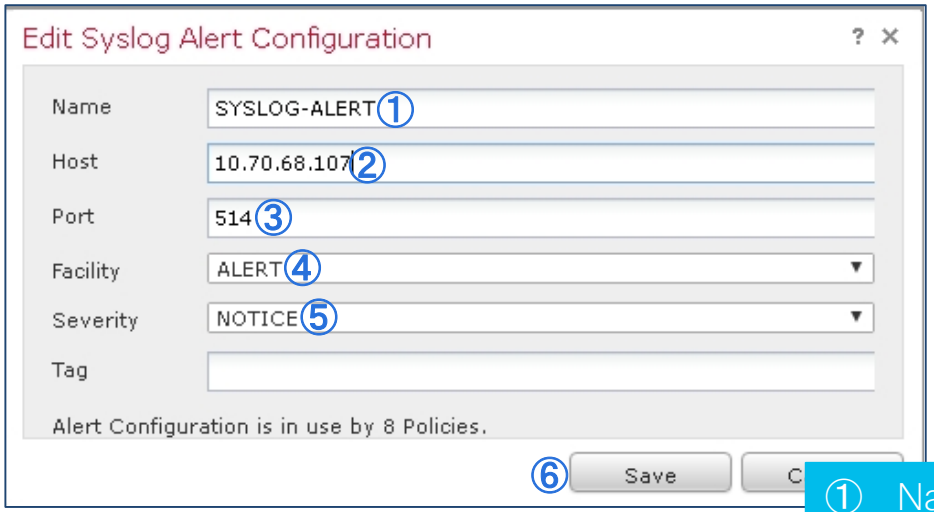


① Policiesを選択
② Actions下のAlertsを選択
③ Create Alertのプルダウンより Create Syslog Alertをクリック

- Create Syslog AlertでEmail、SNMPを選択すると同様にメール、SNMPの設定が可能。

ステップ 2: Syslog Alert作成②

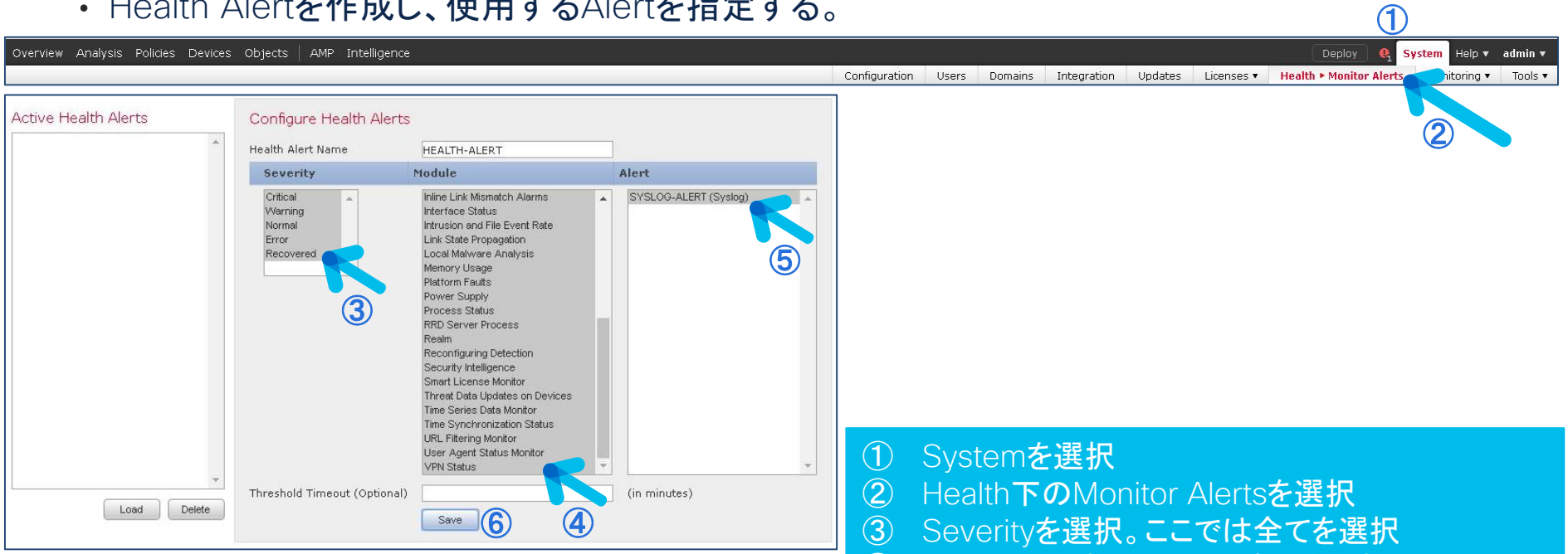
- Syslog Alertを作成



① Nameを入力。ここでは”SYSLOG-ALERT”とする
② HostにSyslogサーバのIPアドレスを入力
③ PortにSyslogサーバのポート番号を入力。デフォルトは514
④ Facilityを選択
⑤ Severityを選択。ここでは”NOTICE”とする
⑥ Saveをクリック

ステップ 3: Health Alert作成とSyslog Alert関連付け

- Health Alertを作成し、使用するAlertを指定する。



① Systemを選択
② Health下のMonitor Alertsを選択
③ Severityを選択。ここでは全てを選択
④ Moduleを選択。ここでは全てを選択
⑤ Alertで作成済みの”SYSLOG-ALERT”を選択
⑥ Saveをクリック

参考: Syslogメッセージの出力例

- 例えばFMCからのメッセージとして、Syslogサーバへは下記のように出力される。

```
Apr 13 01:34:18 FMCv : HMNOTIFY: Threat Data Updates on Devices (Sensor fmc.cs.example.jp): Severity: normal: Process is running correctly
Apr 13 01:34:19 FMCv : HMNOTIFY: AMP for Firepower Status (Sensor fmc.cs.example.jp): Severity: normal: Successfully connected to cloud
Apr 13 01:34:20 FMCv : HMNOTIFY: RRD Server Process (Sensor fmc.cs.example.jp): Severity: normal: The server is functioning normally.
Apr 13 01:34:21 FMCv : HMNOTIFY: Interface Status (Sensor fmc.cs.example.jp): Severity: normal: All interfaces are working correctly
```

参考: その他のアラート設定について①

- 各アラートの設定を行うメニュー画面を記載する。

項目	説明	画面メニュー
Health Monitor Event	機器自体のステータスに関するアラート。	Health Policy ①System>Health>Policy Alert ①Policies>Actions>Alerts Health Alert ①System>Healths>Monitor Alert ②使用するAlertsを一覧より指定
Audit Log Event	監査ログのアラート。	Audit Log ①System>Configuration>Audit Log
Connection Event	Access Control Policyによるコネクションイベントのアラート。	Connection Event ①Policies>Access Control ②アラート有効にするルールの含まれるAccess Control Policyを選択 ③LoggingタブでDefault Syslog Settingsを設定
Discovery Event	Network Discoveryのアラート。	Alert ①Policies>Actions>Alerts Discovery Event Alert ①Policies>Actions>Alerts>Discovery Event Alerts ②使用するAlertsをプルダウンより指定

参考: その他のアラート設定について②

- 各アラートの設定を行うメニュー画面を記載する。

項目	説明	画面メニュー
Impact Flag Alert	Intrusion Policy イベントのうち、 Impact Flagに応じたアラート。	Alert ①Policies>Actions>Alerts Impact Flag Alerts ①Policies>Actions>Alerts>Impact Flag Alerts ②使用するAlertsをプルダウンより指定
Intrusion Event	Intrusion Policyのアラート。	Intrusion Event ①Policies>Access Control>Intrusion ②アラート有効にするIntrusion Policyを選択 ③Advanced Settings>External Responses

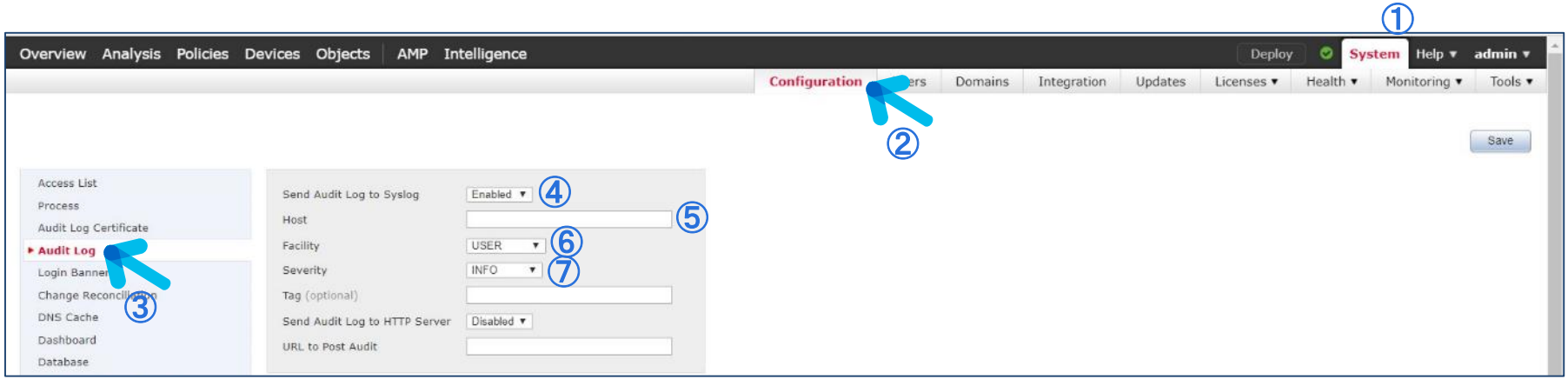
参考: その他のアラート設定について③

- 各アラートの設定を行うメニュー画面を記載する。

項目	説明	画面メニュー
Correlation Event	Correlation Policyのアラート。	Alert ①Policies>Actions>Alerts Correlation Policy ①Policies>Correlation ②アラート有効にするルールの含まれるCorrelation Policyを選択 ③アラート有効にするCorrelation Ruleを選択 ④使用するResponsesをAlert一覧より指定
Network Malware Evert	Network AMPのアラート。	Alert ①Policies>Actions>Alerts Advanced Malware Protection Alert ①Policies>Actions>Alerts>Advanced Malware Protection Alerts ②使用するAlertsをプルダウンより指定

参考: Audit Log Event設定画面

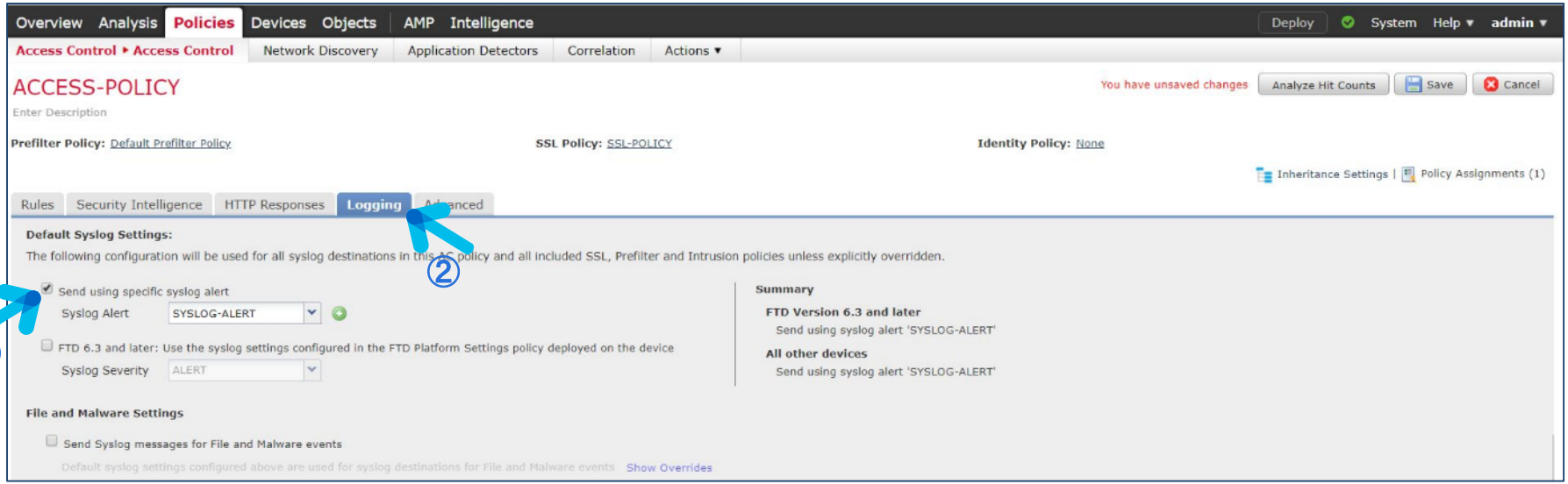
- Audit Log Event設定画面は次のようになる。



① Systemを選択
② Configurationを選択
③ Audit Logを選択
④ プルダウンよりEnableを選択
⑤ SyslogサーバのIPアドレスを入力
⑥ Facilityを選択
⑦ Severityを選択

参考: Connection Event設定画面①

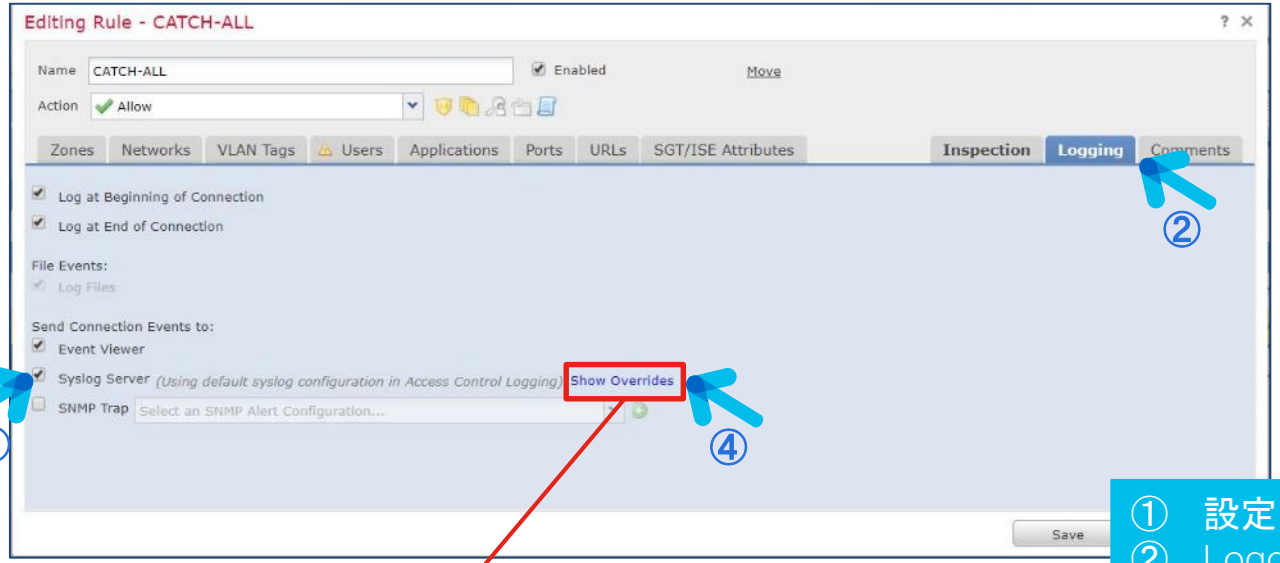
- Connection Event設定画面は次のようになる。

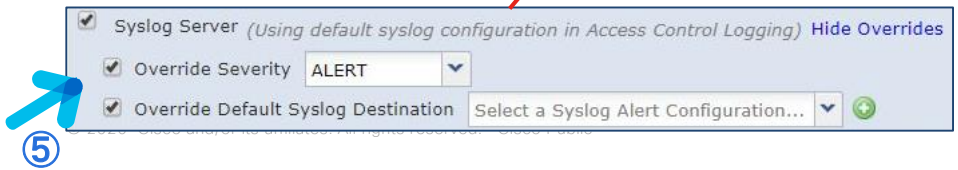


① 設定対象とするAccess policyを開く
② Loggingを選択[Send using specific syslog alert]にチェックを入れる
③ 使用するSyslog Alertをプルダウンより選択

参考: Connection Event設定画面②

- ACP下の特定のAccess Ruleに対し、Syslog設定を個別にOverrideさせることも可能。

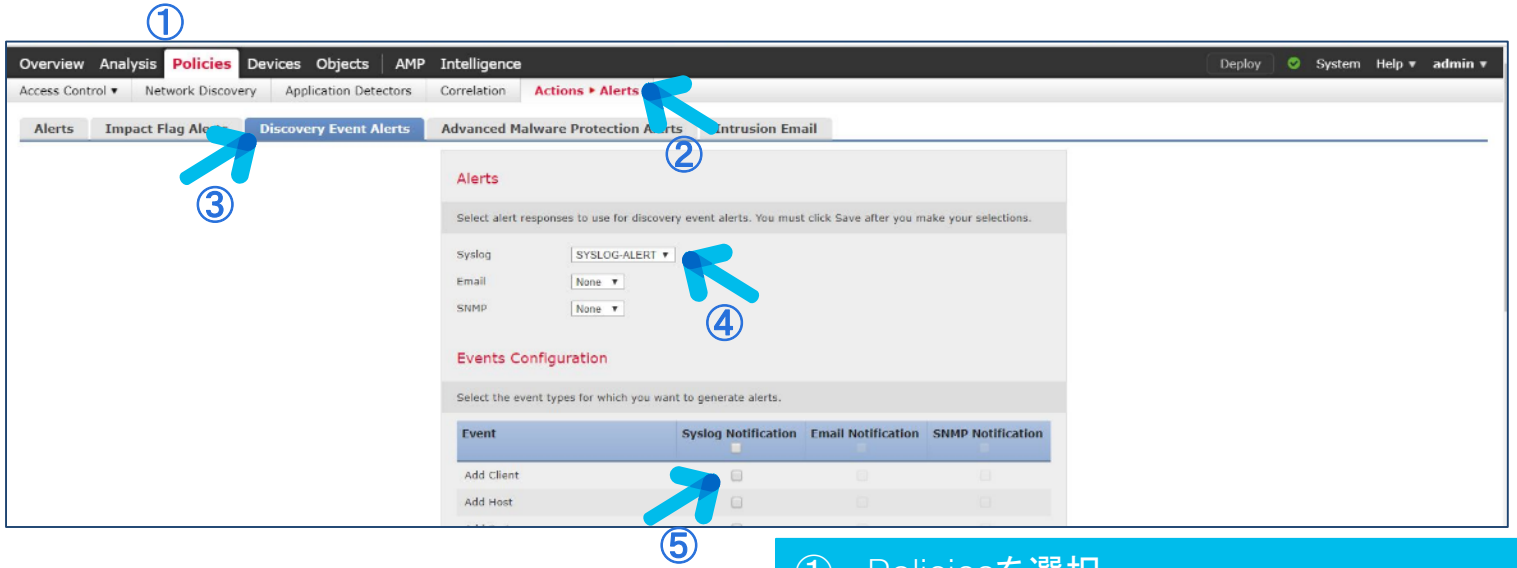




① 設定対象とするAccess Ruleを開く
② Loggingを選択
③ Syslog Serverにチェックを入れる
④ Show Overridesをクリック
⑤ Overrideさせる設定として、Severity、使用するSyslog Alertを指定

参考: Discovery Event設定画面

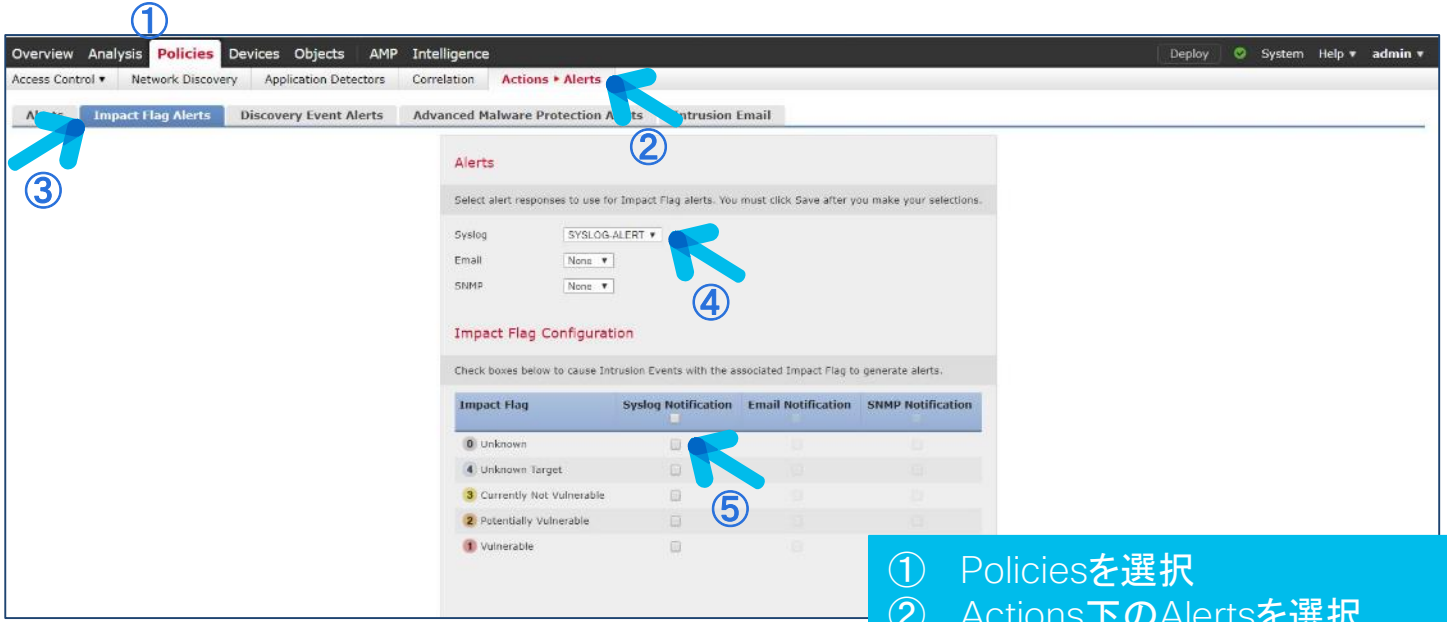
- Discovery Event設定画面は次のようになる。



① Policiesを選択
② Actions下のAlertsを選択
③ Discovery Event Alertsを選択
④ 使用するSyslog Alertをプルダウンより選択
⑤ アラート対象とするイベントへチェックを入れる

参考: Impact Flag Alert設定画面

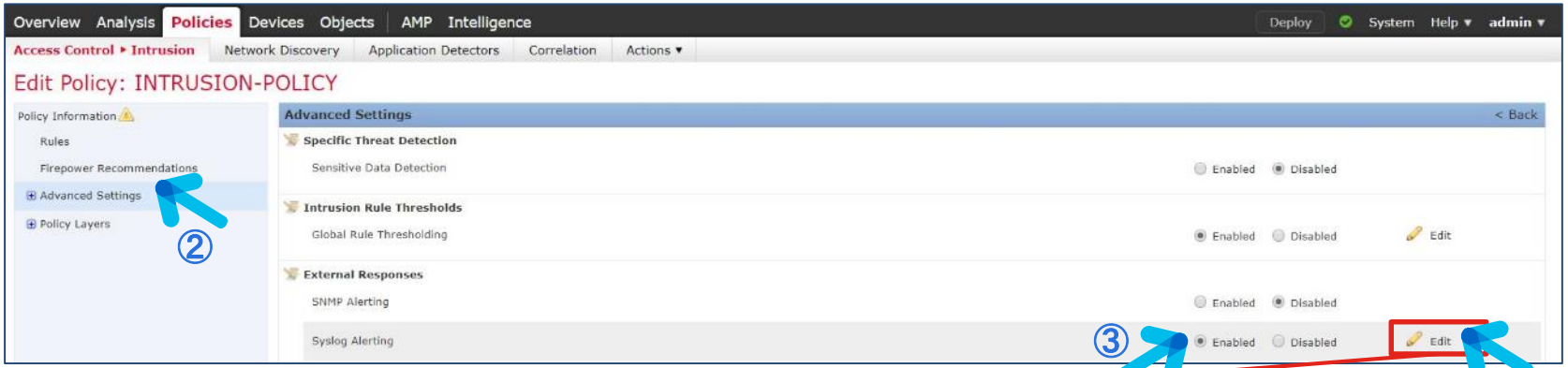
- Impact Flag Alerts設定画面は次のようになる。



① Policiesを選択
② Actions下のAlertsを選択
③ Impact Flag Alertsを選択
④ 使用するSyslog Alertをプルダウンより選択
⑤ アラート対象とするImpact Flagへチェックを入れる

参考: Intrusion Event設定画面

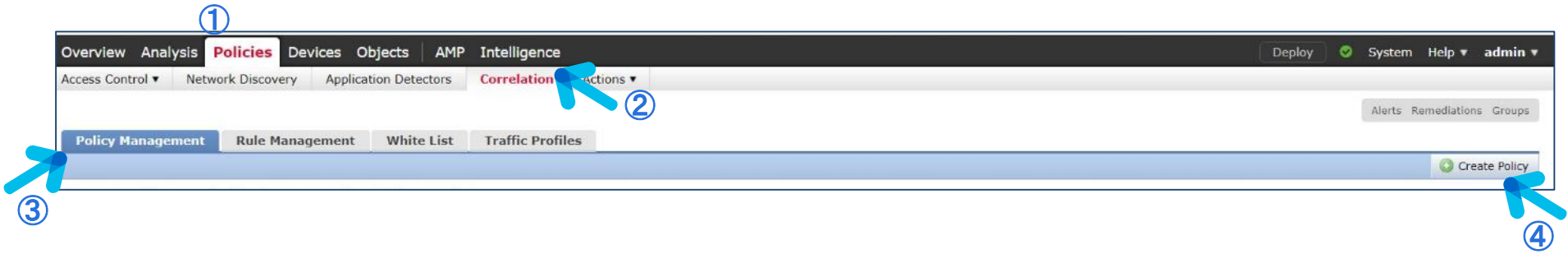
- Intrusion Event設定画面は次のようになる。



① 設定対象とするintrusion Policyを開く
② Advanced Settingsを選択
③ Syslog AlertingのEnabledへチェックを入れる
④ Editをクリック
⑤ Intrusion Policyを関連付けるAccess Policyと同じ
Syslogサーバから変更する場合、Syslogサーバを指定
⑥ Facility、Severityを指定

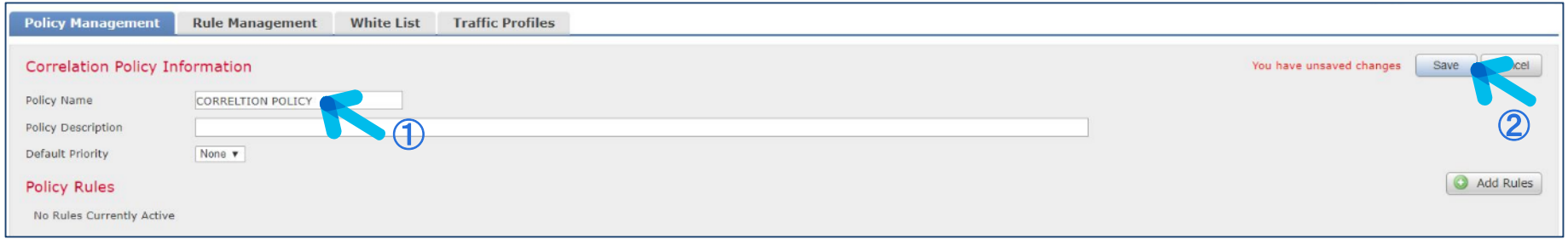
参考: Correlation Event設定画面 Correlation Policy作成①

- Correlation Policyを設定することで、詳細な条件に基づくアラート通知を行える。



① Policiesを選択
② Correlationを選択
③ Policy Managementを選択
④ Create Policyをクリック

参考: Correlation Event設定画面 Correlation Policy作成②

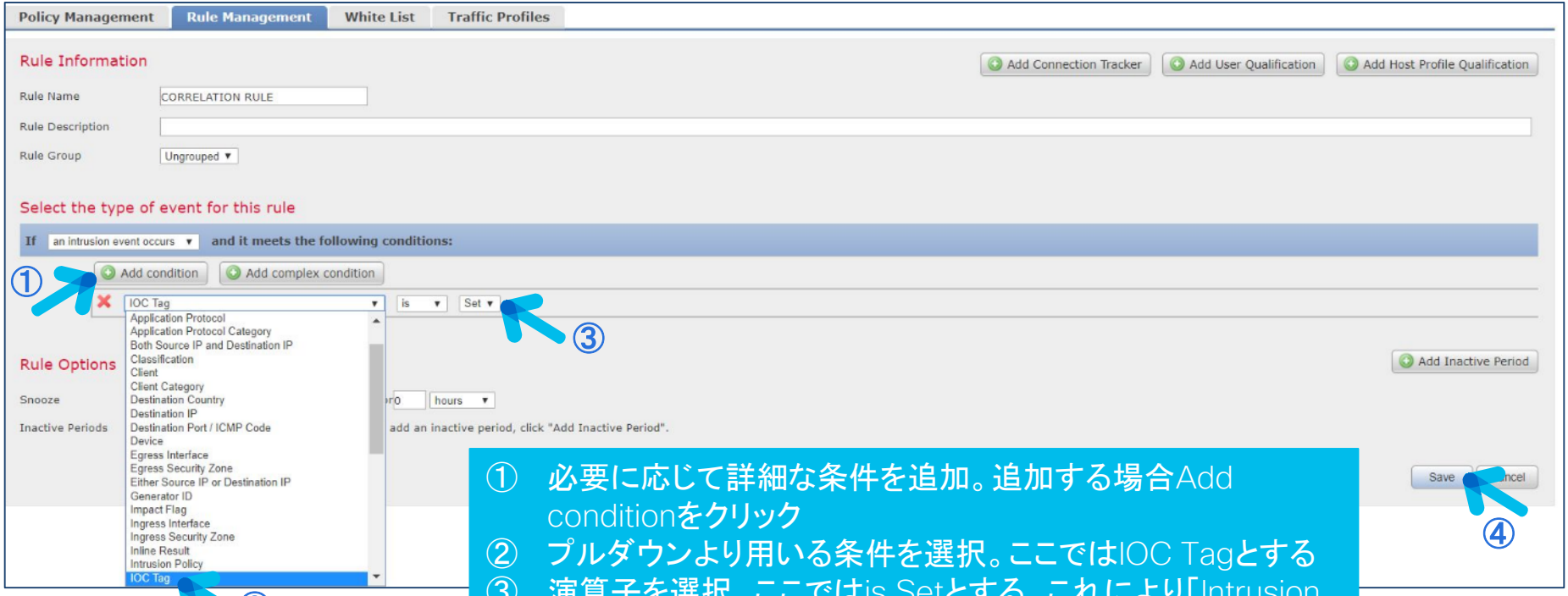


① Policy Nameを入力。ここでは”CORRELATION POLICY”とする
② Saveをクリック

参考: Correlation Event設定画面 Correlation Rule作成①

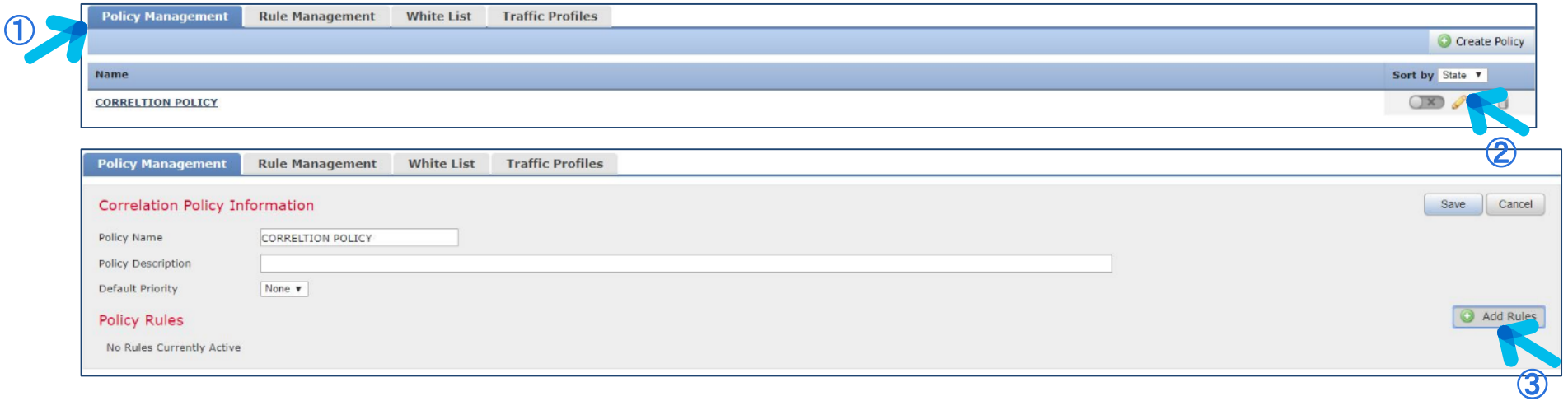
① Rule Nameを入力。ここでは”CORRELATION RULE”とする
② プルダウンよりCorrelation Policyによりアラート通知させる場合の、条件を選択する。ここではan intrusion event occursとする

参考: Correlation Event設定画面 Correlation Rule作成②



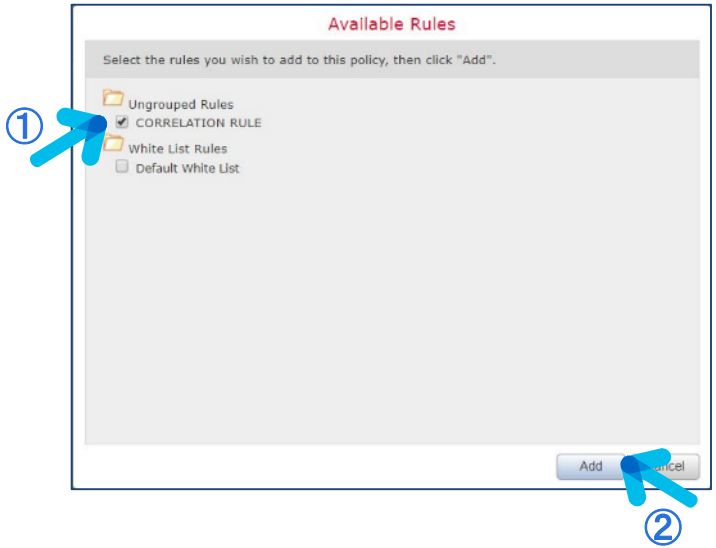
① 必要に応じて詳細な条件を追加。追加する場合Add conditionをクリック
② プルダウンより用いる条件を選択。ここではIOC Tagとする
③ 演算子を選択。ここではis Setとする。これにより「Intrusion Eventが発生し、なおかつそれにIOC Tagがセットされていたら」という条件になる。
④ Saveをクリック

参考: Correlation Event設定画面 Correlation Policy設定③



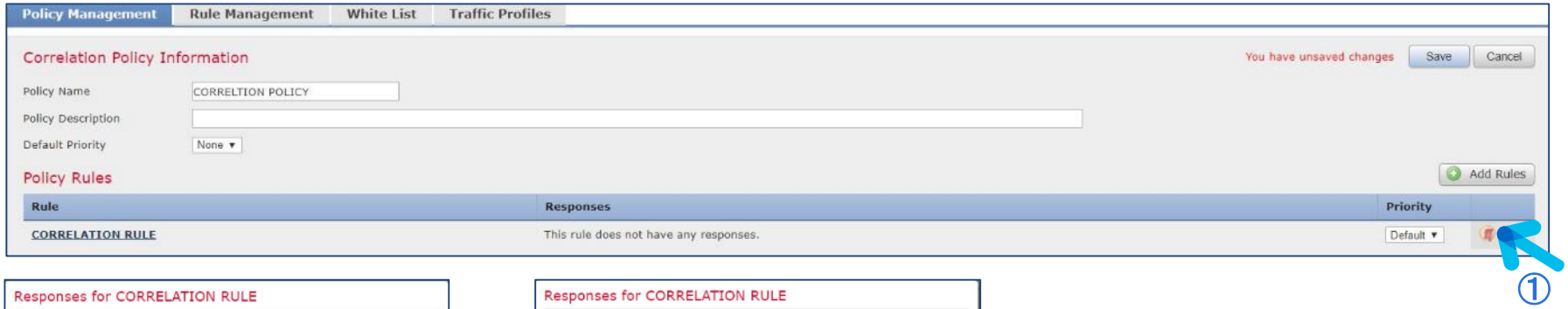
① Policy Managementを選択
② 鉛筆マークをクリック
③ Add Ruleをクリック

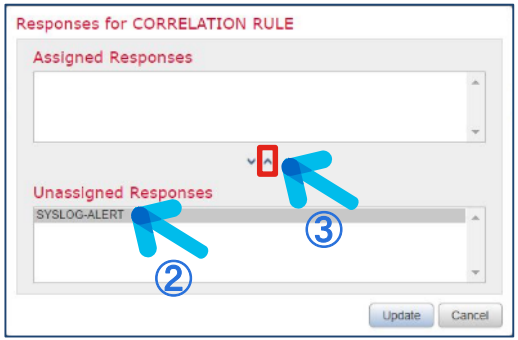
参考: Correlation Event設定画面 Correlation Policy設定④



① Correlation Policyへ含めるRuleへチェックを入れる。
② Addをクリック

参考: Correlation Event設定画面 アラートの追加①





① Responsesアイコンをクリック
② Correlation Ruleで使用する Syslog Alertを選択
③ 追加アイコンをクリック
④ Updateをクリック

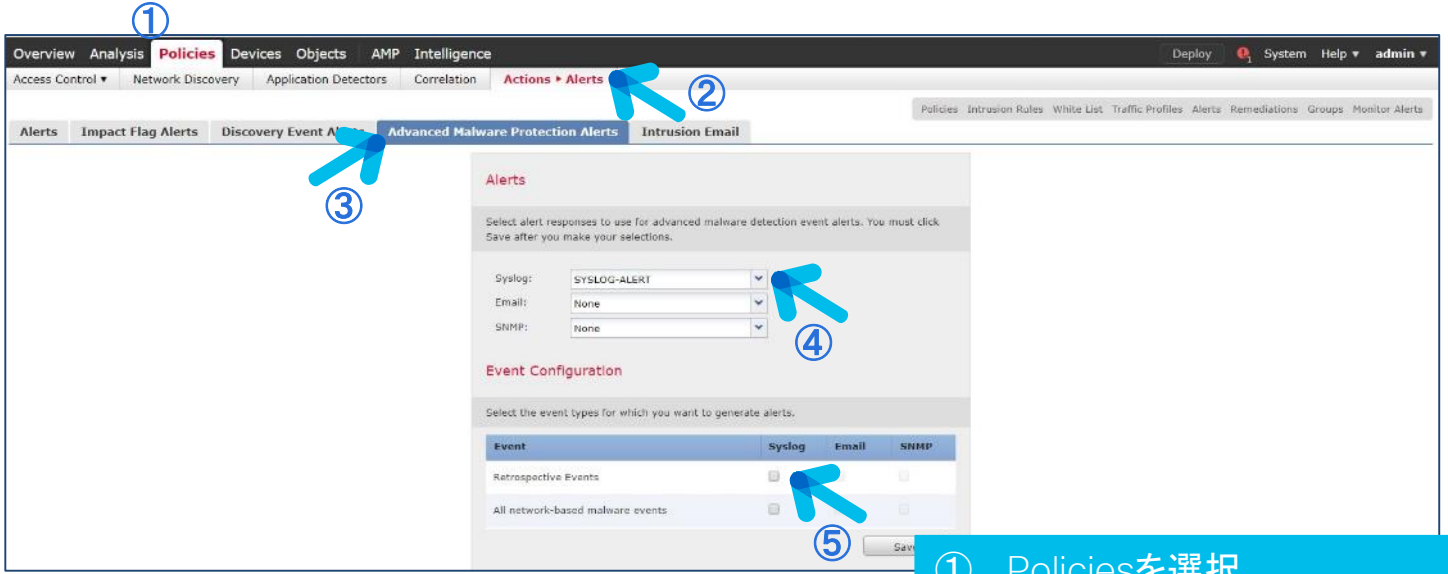
参考: Correlation Event設定画面 アラートの追加②

① Activateアイコンをクリック。これによってCorrelation Policyが有効になり、Correlation Ruleの条件を満たすイベントが発生した場合にアラートが送信される

- Correlation Ruleの条件文については下記を参照のこと
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/correlation_policies.html

参考: Network Malware Evert設定画面

- Network Malware Evert設定画面は次のようになる。

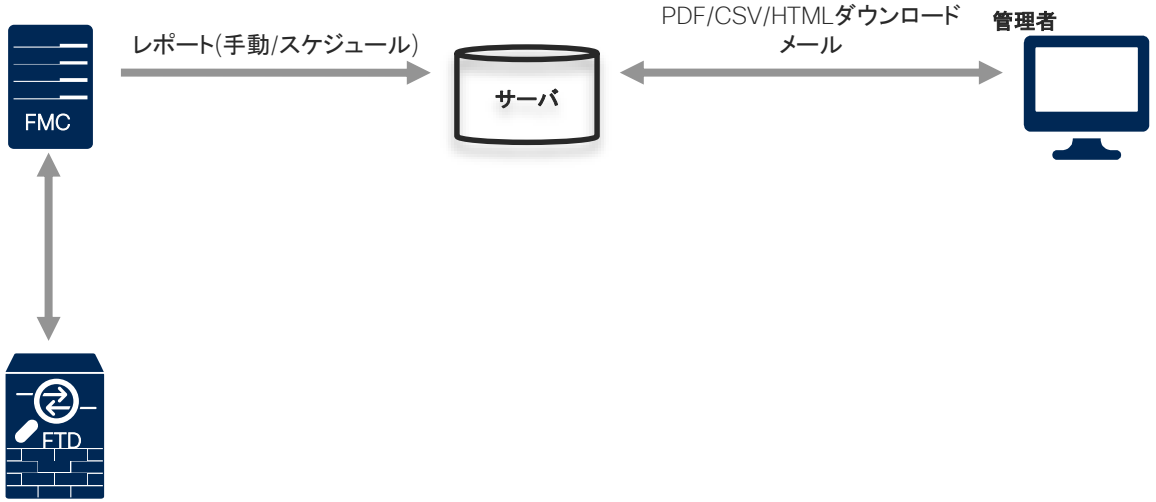


① Policiesを選択
② Actions下のAlertsを選択
③ Advanced Malware Protection Alertsを選択
④ 使用するSyslog Alertをプルダウンより選択
⑤ アラート対象とするEventへチェックを入れる

レポーティング

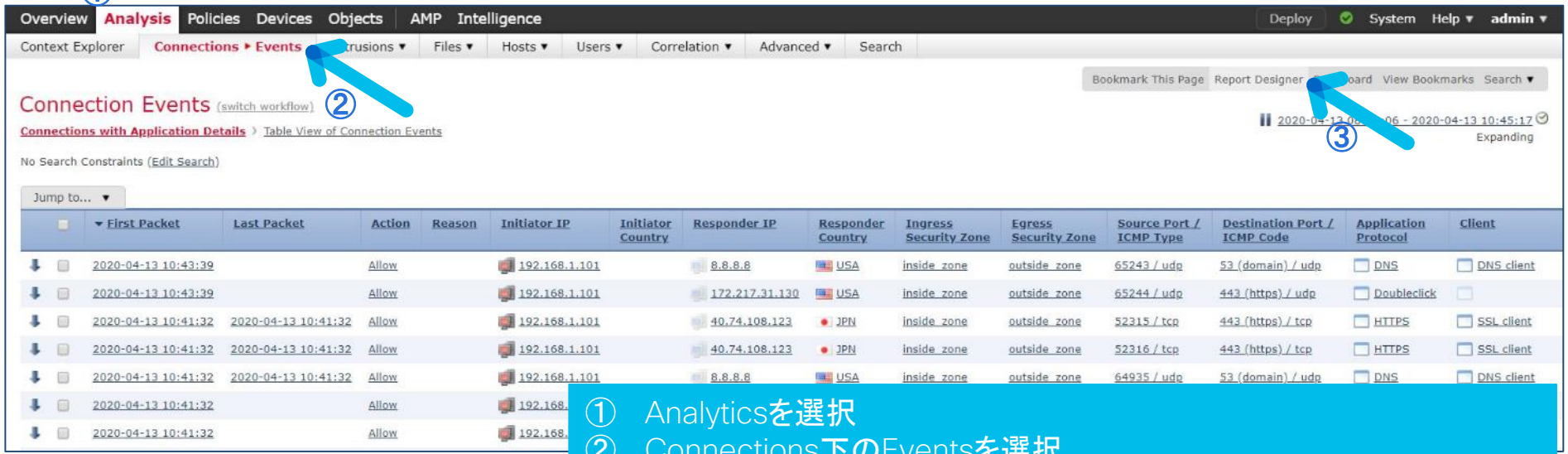
レポート機能

- FMCより手動、もしくはスケジュールでレポートを生成できる。
- またレポートに含める内容はカスタマイズすることも可能。



ステップ 1-1:手動レポート生成①

・レポートの生成対象とする画面を開く。ここではConnection Eventを例にする。

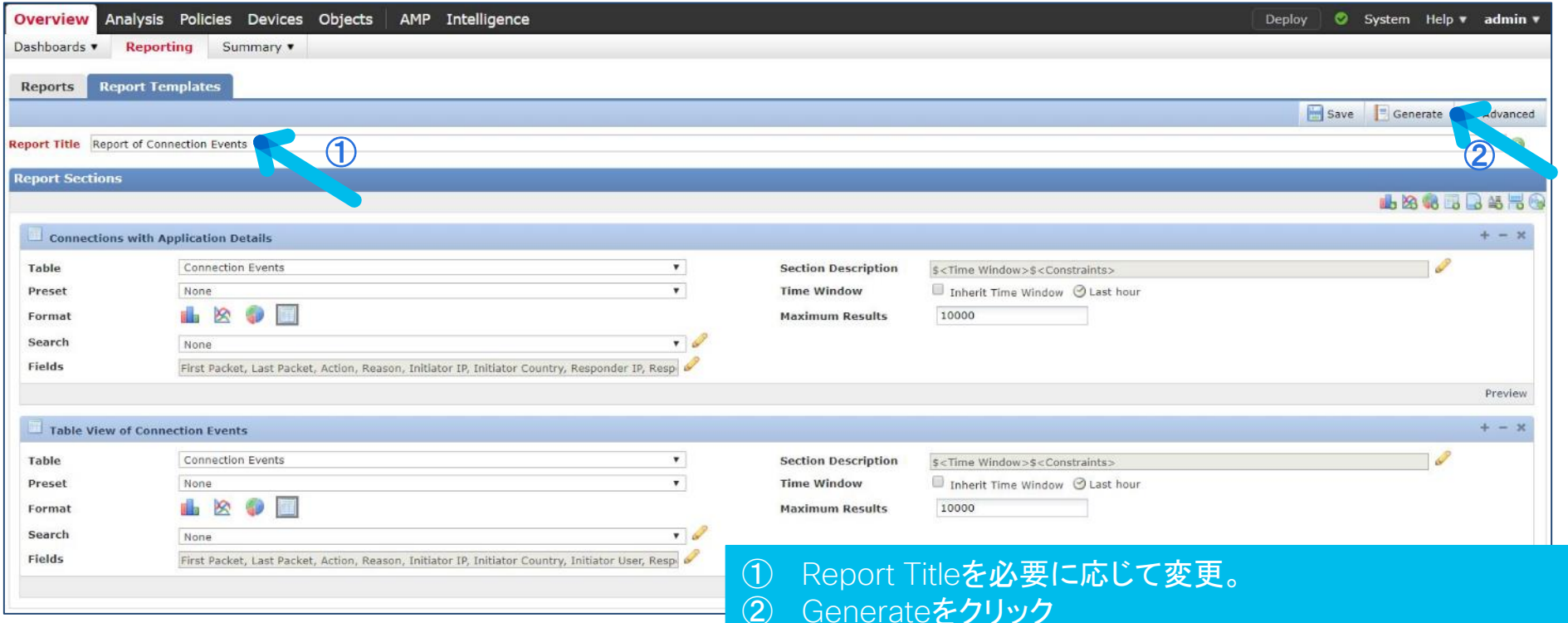


① Analyticsを選択
② Connections下のEventsを選択
③ Report Designerをクリック

- その他のイベントも同様に、Report Designerをクリックすることでレポートを手動で生成できる。

ステップ 1-1:手動レポート生成②

- 手動生成レポートのパラメータを指定する。



① Report Titleを必要に応じて変更。
② Generateをクリック

ステップ 1-1:手動レポート生成③

- 手動生成レポートの出力形式を指定する。

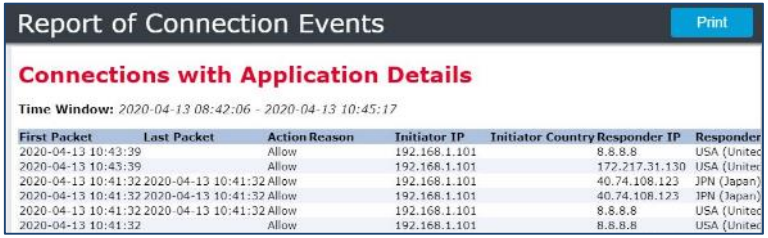
① File NameはReport Titleが引き継がれる。変更することも可能
② Output Formatを選択。HTML、PDF、CSV。
③ 必要に応じてRelay Hostにてレポートを送信するMail Relay Hostを指定する。
④ Generateをクリック

ステップ 1-2:レポートの確認①

- 生成したレポートの確認。

① Reportsを選択。この画面は生成済みレポートの一覧を表示している
② 確認する対象のレポートのTime Completedの欄に日時が表示されていることを確認。日時が表示されていれば、レポートの生成処理が完了している
③ 確認対象のレポートにチェックを入れる
④ Downloadをクリック

ステップ 1-2:レポートの確認②


Report of Connection Events

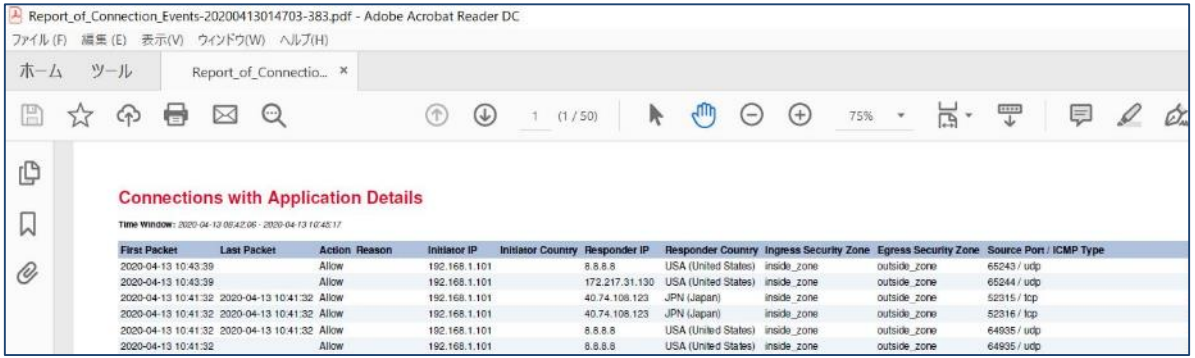
Print

Connections with Application Details

Time Window: *2020-04-13 08:42:06 - 2020-04-13 10:45:17*

First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder
2020-04-13 10:43:39		Allow		192.168.1.101		8.8.8.8	USA (United
2020-04-13 10:43:39		Allow		192.168.1.101		172.217.31.130	USA (United
2020-04-13 10:41:32	2020-04-13 10:41:32	Allow		192.168.1.101		40.74.108.123	JPN (Japan)
2020-04-13 10:41:32	2020-04-13 10:41:32	Allow		192.168.1.101		40.74.108.123	JPN (Japan)
2020-04-13 10:41:32	2020-04-13 10:41:32	Allow		192.168.1.101		8.8.8.8	USA (United
2020-04-13 10:41:32		Allow		192.168.1.101		8.8.8.8	USA (United

HTML形式


Report_of_Connection_Events-20200413014703-383.pdf - Adobe Acrobat Reader DC

ファイル (F) 編集 (E) 表示(V) ウィンドウ(W) ヘルプ(H)

ホーム ツール Report_of_Connectio... ×

1 (1 / 50) 75%

Connections with Application Details

Time Window: *2020-04-13 08:42:06 - 2020-04-13 10:45:17*

First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type
2020-04-13 10:43:39		Allow		192.168.1.101		8.8.8.8	USA (United States)	inside_zone	outside_zone	65243 / udp
2020-04-13 10:43:39		Allow		192.168.1.101		172.217.31.130	USA (United States)	inside_zone	outside_zone	65244 / udp
2020-04-13 10:41:32	2020-04-13 10:41:32	Allow		192.168.1.101		40.74.108.123	JPN (Japan)	inside_zone	outside_zone	52315 / tcp
2020-04-13 10:41:32	2020-04-13 10:41:32	Allow		192.168.1.101		40.74.108.123	JPN (Japan)	inside_zone	outside_zone	52316 / tcp
2020-04-13 10:41:32	2020-04-13 10:41:32	Allow		192.168.1.101		8.8.8.8	USA (United States)	inside_zone	outside_zone	64935 / udp
2020-04-13 10:41:32		Allow		192.168.1.101		8.8.8.8	USA (United States)	inside_zone	outside_zone	64935 / udp

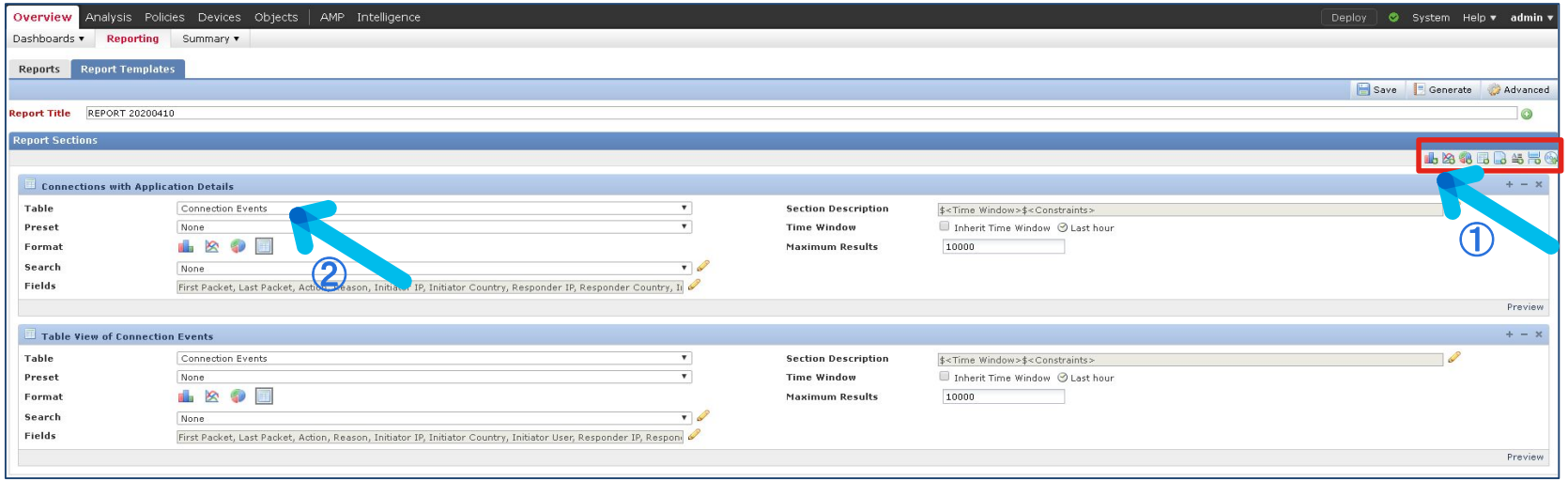
PDF形式

	A	B	C	D	E	F	G	H	I	J	K
1	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type
2	2020/4/13 10:43		Allow		192.168.1.101		8.8.8.8	USA (United States)	inside_zone	outside_zone	65243 / udp
3	2020/4/13 10:43		Allow		192.168.1.101		172.217.31.130	USA (United States)	inside_zone	outside_zone	65244 / udp
4	2020/4/13 10:41	2020/4/13 10:41	Allow		192.168.1.101		40.74.108.123	JPN (Japan)	inside_zone	outside_zone	52315 / tcp
5	2020/4/13 10:41	2020/4/13 10:41	Allow		192.168.1.101		40.74.108.123	JPN (Japan)	inside_zone	outside_zone	52316 / tcp
6	2020/4/13 10:41	2020/4/13 10:41	Allow		192.168.1.101		8.8.8.8	USA (United States)	inside_zone	outside_zone	64935 / udp
7	2020/4/13 10:41		Allow		192.168.1.101		8.8.8.8	USA (United States)	inside_zone	outside_zone	64935 / udp

CSV形式

参考:レポートのカスタマイズ

- レポートはセクションの追加や変更といったカスタマイズができる。

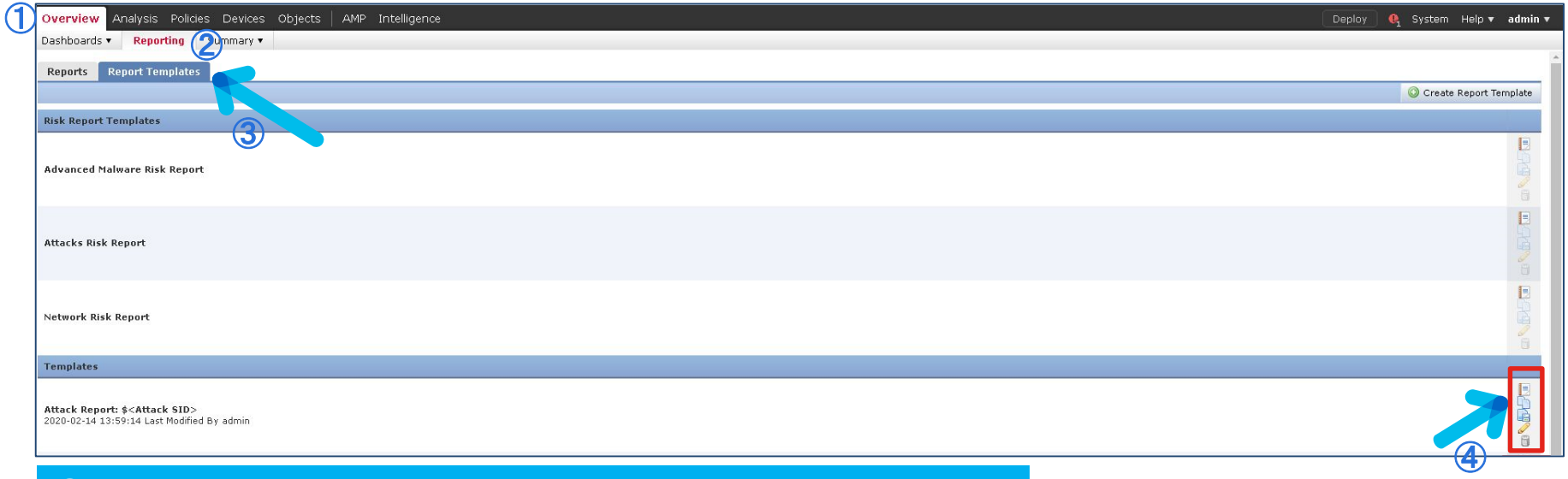


① **追加するセクション種別の選択。**Bar Chart / Line Chart / Pie Chart / Table View / Detail View / Text Section / Page Break / Import Sections from Dashboard, Summaries, and Workflows**より指定。**

② **セクションごとのカスタマイズも可能。**Table**種別**(Table)**、レポートに含める検索条件**(Search)**、レポート対象の期間**(Time Window)**、グラフの**X/Y**軸**((X-Axis/Y-Axis)**など。**

参考:レポートテンプレートの管理

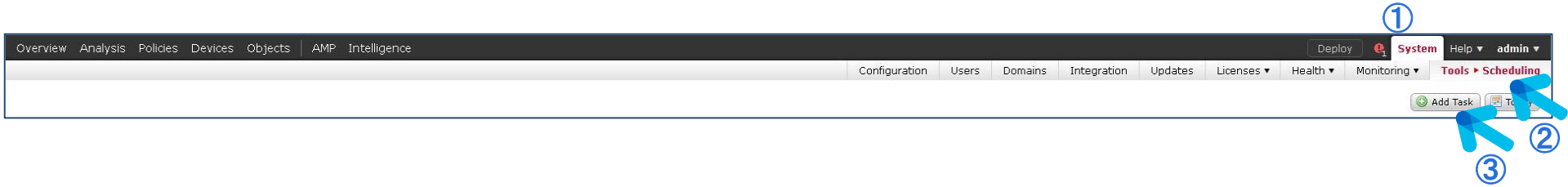
- デフォルト定義のもの、カスタム定義したものともにテンプレート一覧より管理できる。



① Overviewを選択
② Reportingを選択
③ Report Templatesを選択
④ 各種操作を実行可能。Generate / Copy / Export / Edit / Delete
※ただしRisk Report Templets下のものはGenerateのみ。

ステップ 2-1:スケジュール レポート生成①

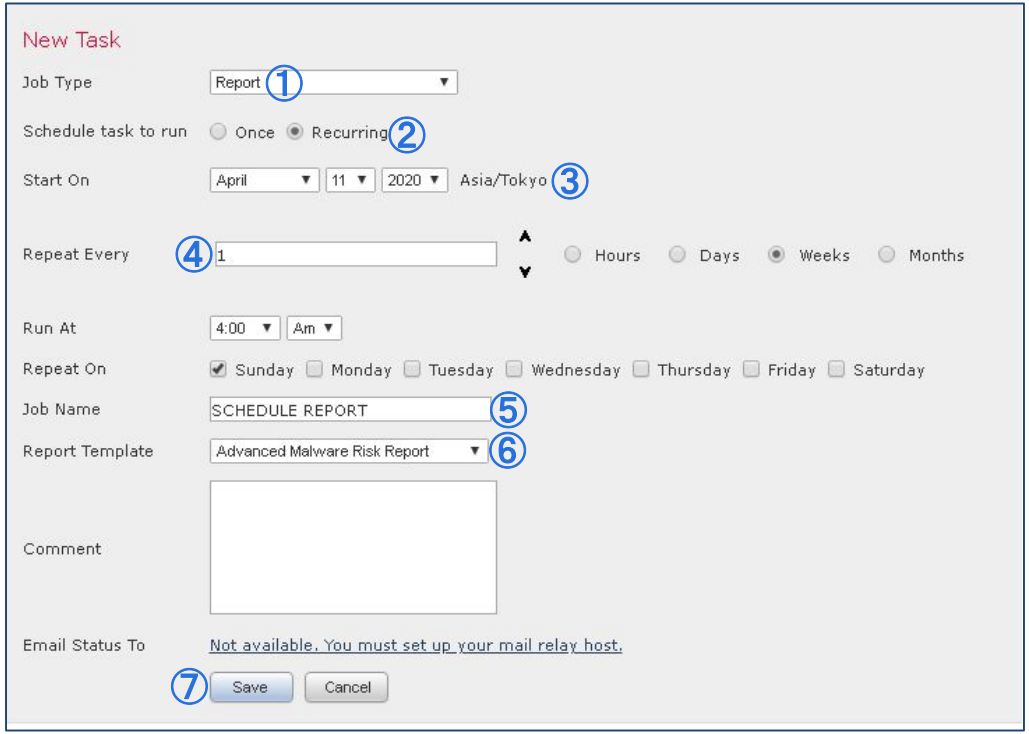
- スケジュールタスクにて、レポート生成タスクを定義する。



① Systemを選択
② Tools下のSchedulingを選択
③ Add Taskをクリック

ステップ 2-1:スケジュール レポート生成②

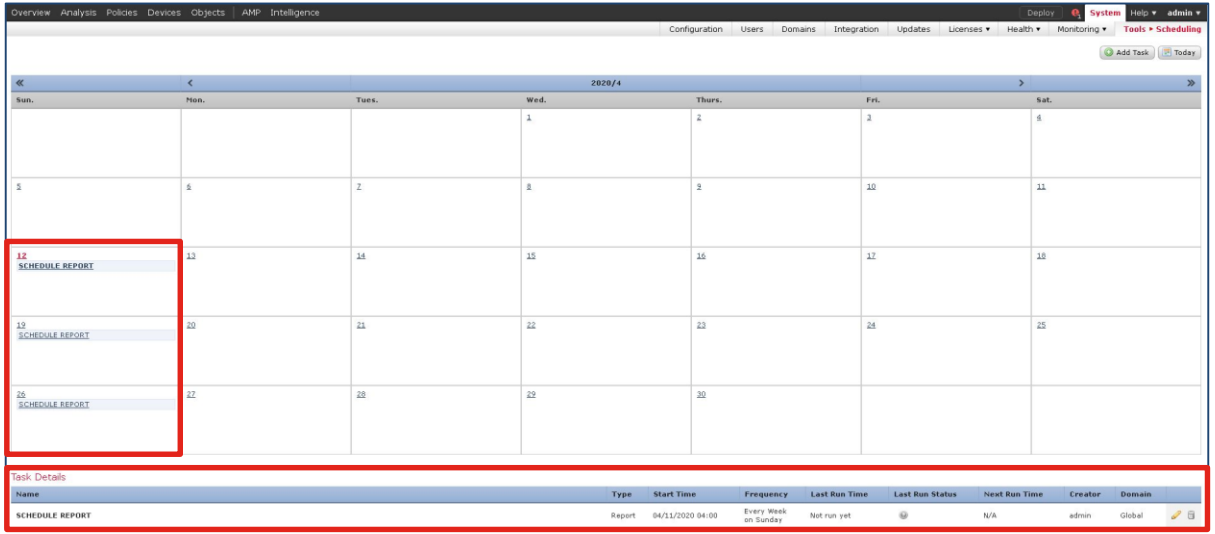
- スケジュールタスクにて、レポート生成タスクを定義する。



① プルダウンよりReportをを選択
② Recurringへチェックを入れる
③ レポート生成タスクの開始年月日を指定。ここでは2020年4月11日とする。
④ レポート生成タスクの頻度を指定。ここでは週次とし、毎週日曜日の午前4:00に処理を開始する設定をしている
⑤ Job Nameを入力。ここでは”SCHEDULE REPORT”とする
⑥ 生成するReport Templateを指定する
⑦ Saveをクリック

ステップ 2-1:スケジュール レポート確認

- スケジュールタスクにて、レポート生成タスクが保存されている。



- 設定した通りにタスクが保存されていることを確認する。先の例で2020年4月11日以降の毎週日曜日と設定したため、赤枠部分のようになっている。
- 各タスクをクリックするとTask Detailsが表示される。ここからタスクの実行状況や、編集/削除の操作を実行できる。
- 生成されたレポートは手動生成レポートと同様に、Reports(Overview > Reporting > Reports)より確認が可能。

参考: テンプレート定義済みレポートを日本語で生成

- テンプレート定義済みのレポートは即時生成が可能。また、UIを日本語化していれば日本語でのレポート生成が可能。UI日本語化の方法は以下の通り

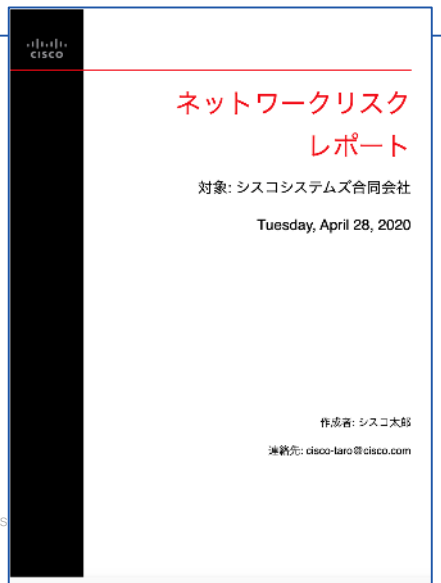
① System > Configurationをクリック
② Languageをクリック
③ “日本語” を選択
④ Saveをクリック

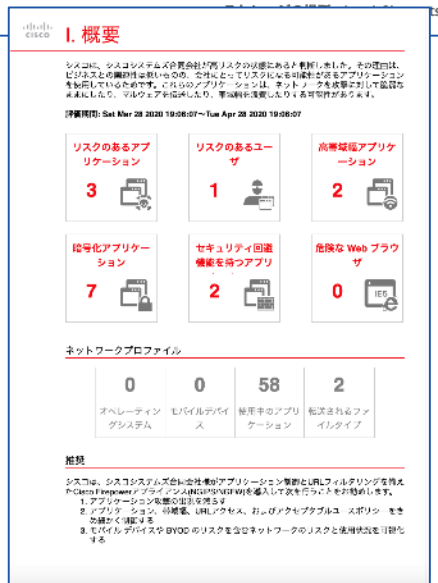
参考: テンプレート定義済みレポートを日本語で生成(続き)

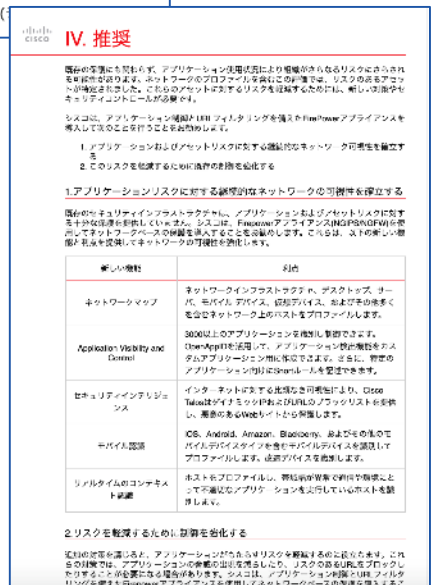
※パラメータに日本語を利用可能

参考: テンプレート定義済みレポートを日本語で生成(続き)

※日本語への翻訳品質は高評価



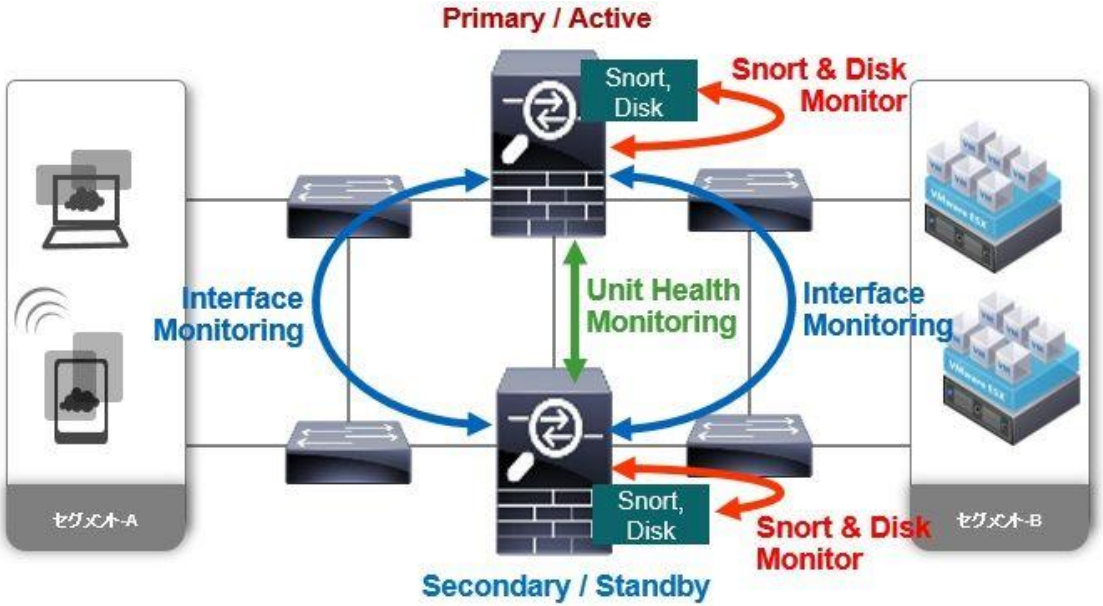




13. FTD High Availabilityの設定

FTD High Availability (HA) について

- FTDでは高可用性の実現のためにアクティブ/スタンバイフェイルオーバーをサポート

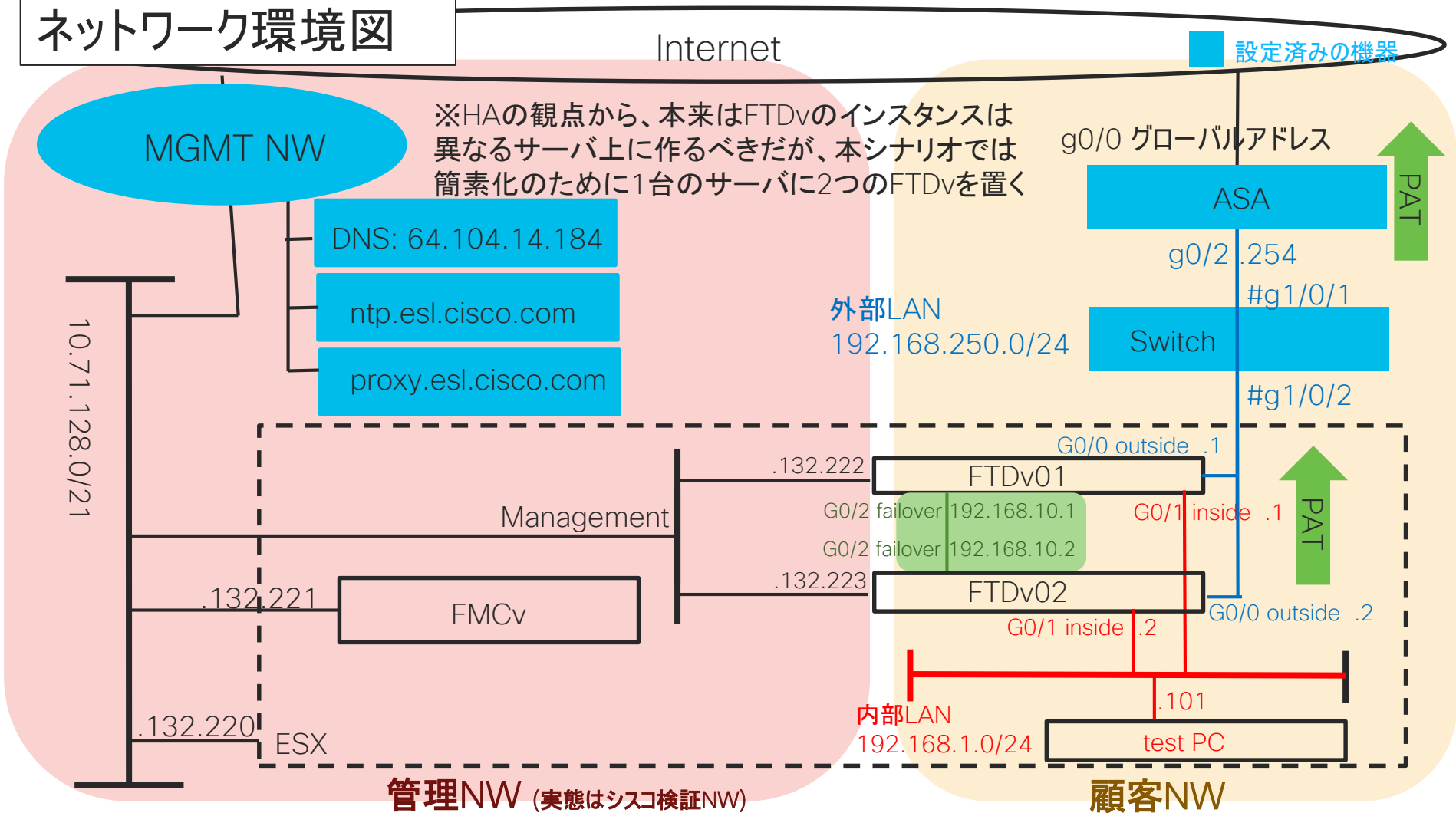


- 設定・動作イメージはASA HAと同様
- FTDではヘルスモニタリングとしてインタフェース以外に、Snortプロセスや Diskの障害監視も実施
- AWS等パブリッククラウド上にデプロイされたFTDvはHA非サポート

HA設定における事前確認事項

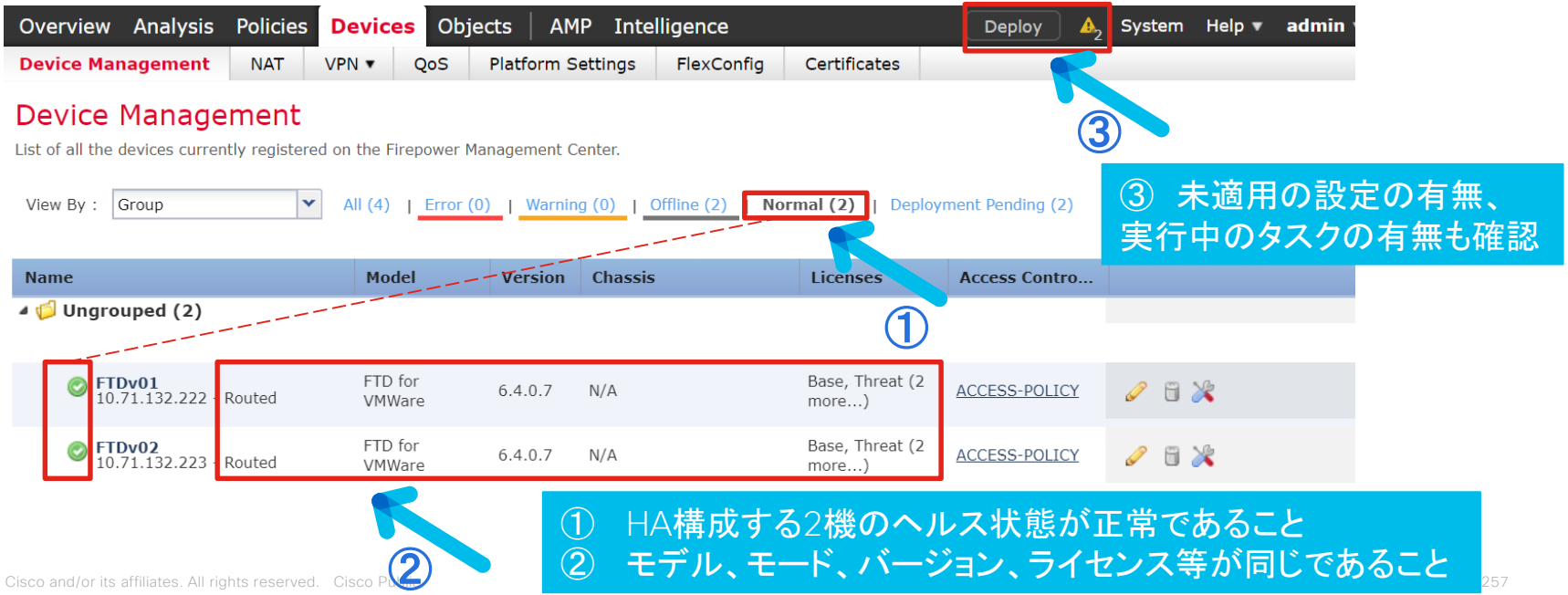
- 同じモデルあること
- 同じインターフェイス数とインターフェイスタイプであること。モジュール利用時は、同じモジュールを各デバイスに装着すること
- 同じソフトウェアバージョンを利用していること
- 同じ firewallモードであること。Routed(default)、もしくは Transparent
- DHCPや PPPoE設定をインターフェイスにしてないこと。DHCPのアドレス割当てや PPPoE接続情報は、同期非サポートのため
- ヘルスモニターのステータスが各デバイスでNormal(正常)であること
- すべての設定変更が各デバイスでデプロイ済みであること
- 2台分のライセンスを用意すること。FTD HAでは、各デバイスに同じライセンス割当が必要のため、例えばIPS機能を使う場合は、Threatライセンスが2つ必要。HA 構成での購入時にディスカウントされたバンドル型番有り。なお、Baseライセンスのみは各FTDデバイス内に同梱されており自動使用されるため準備は不要
- 既に稼働中のFTDデバイス(スタンドアローン)に、新規FTDデバイスを追加し冗長ペアを組む場合、通信影響の少ない時間帯や メンテナンスタイムに実施すること。FTD HAを組む際、Snort自動再起動が発生し、通信影響が発生するため

ネットワーク環境図

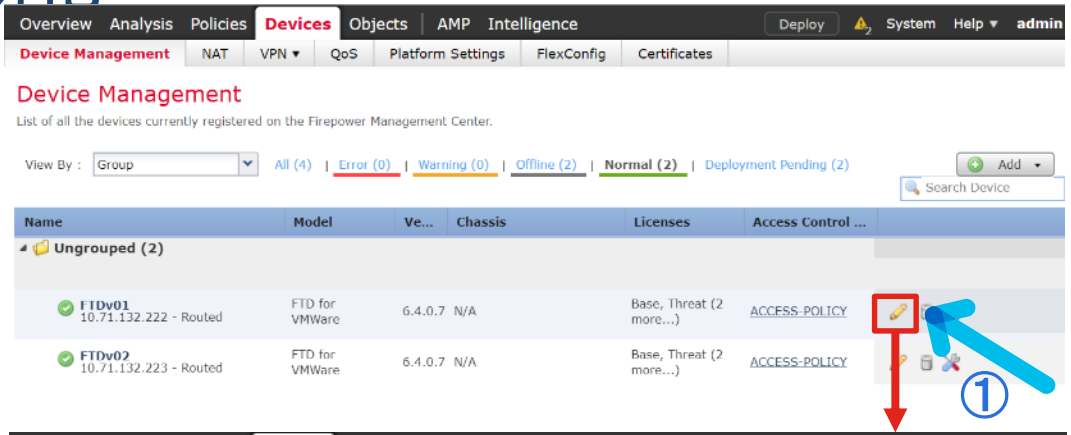

Internet
設定済みの機器
※HAの観点から、本来はFTDvのインスタンスは
異なるサーバ上に作るべきだが、本シナリオでは
簡素化のために1台のサーバに2つのFTDvを置く
MGMT NW
DNS: 64.104.14.184
ntp.esl.cisco.com
proxy.esl.cisco.com
10.71.128.0/21
g0/0 グローバルアドレス
ASA
PAT
g0/2 .254
#g1/0/1
外部LAN
192.168.250.0/24
Switch
#g1/0/2
G0/0 outside .1
.132.222
FTDv01
Management
G0/2 failover 192.168.10.1
G0/1 inside .1
PAT
G0/2 failover 192.168.10.2
.132.223
FTDv02
.132.221
FMCv
G0/0 outside .2
G0/1 inside .2
.101
内部LAN
192.168.1.0/24
test PC
.132.220
ESX
管理NW (実態はシスコ検証NW)
顧客NW

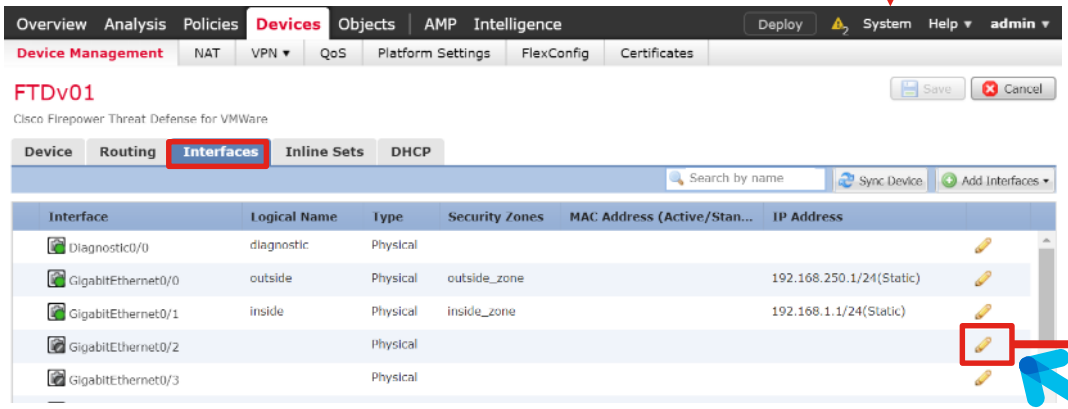
ステップ1-1: HA設定 – 事前準備・確認

- HA構成のためにFTDv02を新たにインストールし、初期セットアップおよびFMCへの管理登録を実施（手順はFTDv01と同様）
- HA構成するFTDの状態が問題ないことを確認

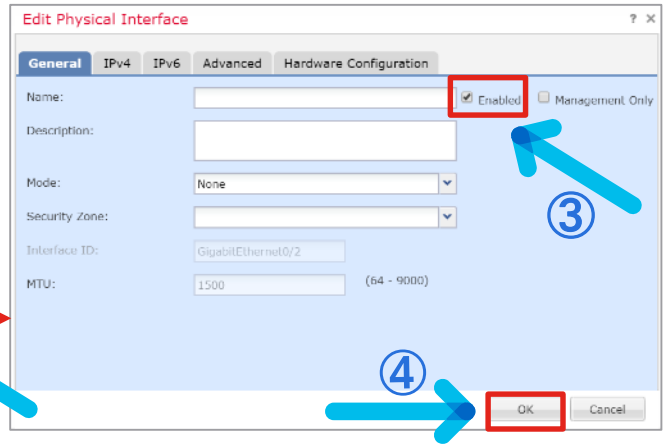


ステップ2-1: HA設定 – FTDv01のHAリンクのためのIF有効化



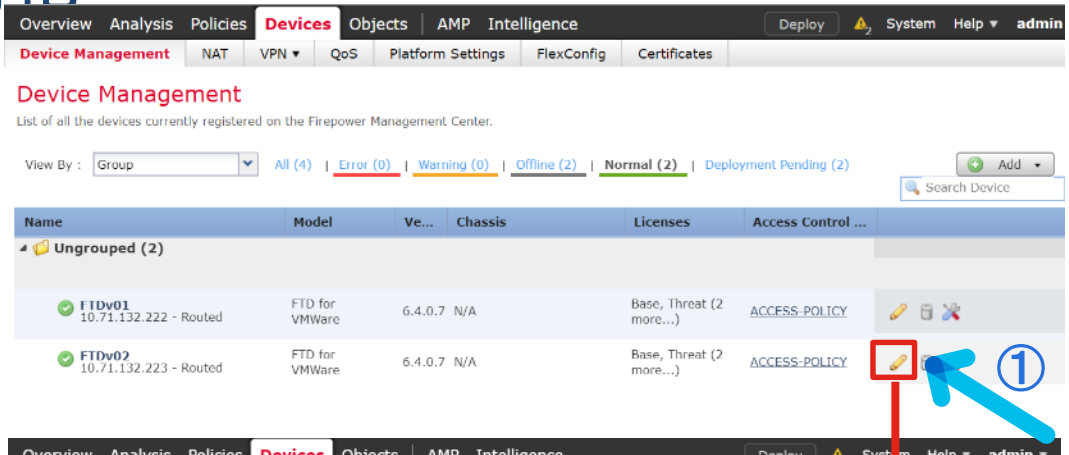


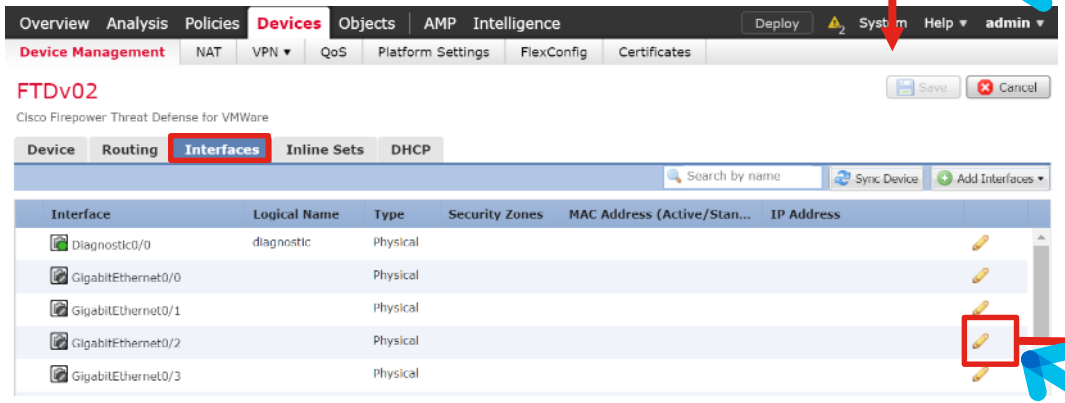
① Device ManagementよりFTDv01の鉛筆マークをクリック
② Interfaceタブをクリックし、Gig0/2の鉛筆マークをクリック
③ GenaralのEnableにチェック
④ OKをクリック
⑤ Saveをクリックして設定を保存

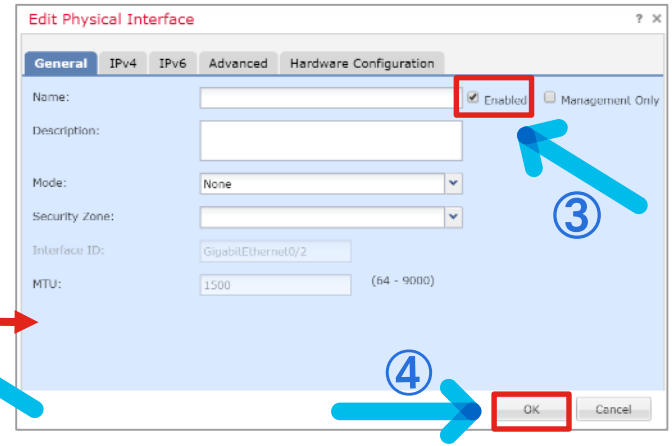


注：ESXiでHAリンク接続用の仮想スイッチを別途作成必要

ステップ2-2: HA設定 – FTDv02のHAリンクのためのIF有効化



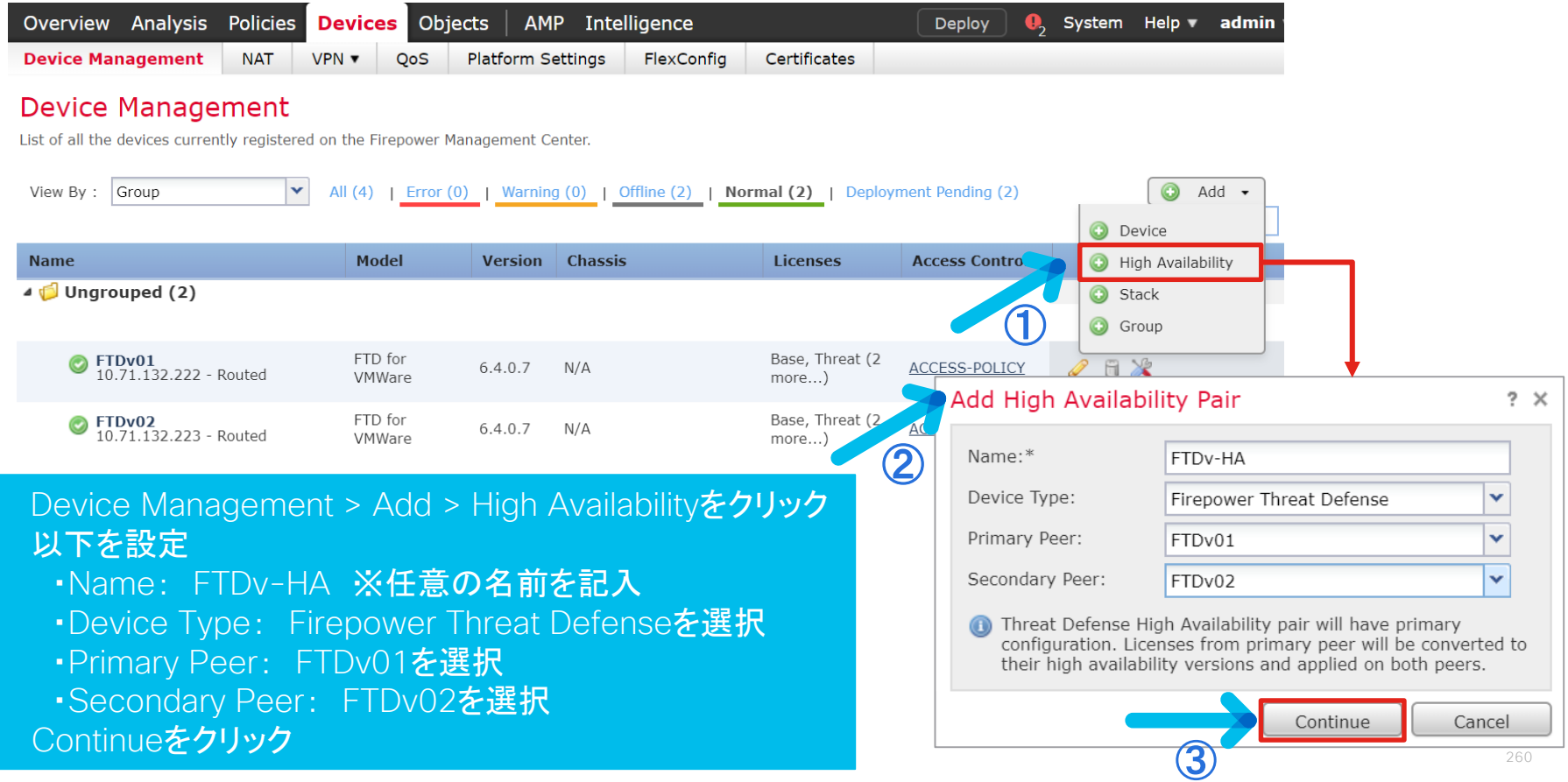




① Device ManagementよりFTDv02の鉛筆マークをクリック
② Interfaceタブをクリックし、Gig0/2の鉛筆マークをクリック
※他のIFはHAに成功すれば自動でEnableとなるため事前設定不要
③ GenaralのEnableにチェック
④ OKをクリック
⑤ Saveをクリックして設定を保存
⑥ DeployをクリックしてFTDに適用

注：ESXiでHAリンク接続用の仮想スイッチを別途作成必要

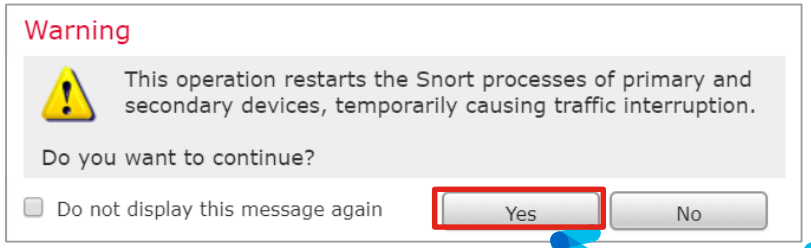
ステップ3-1: HA設定 – HAペアの作成



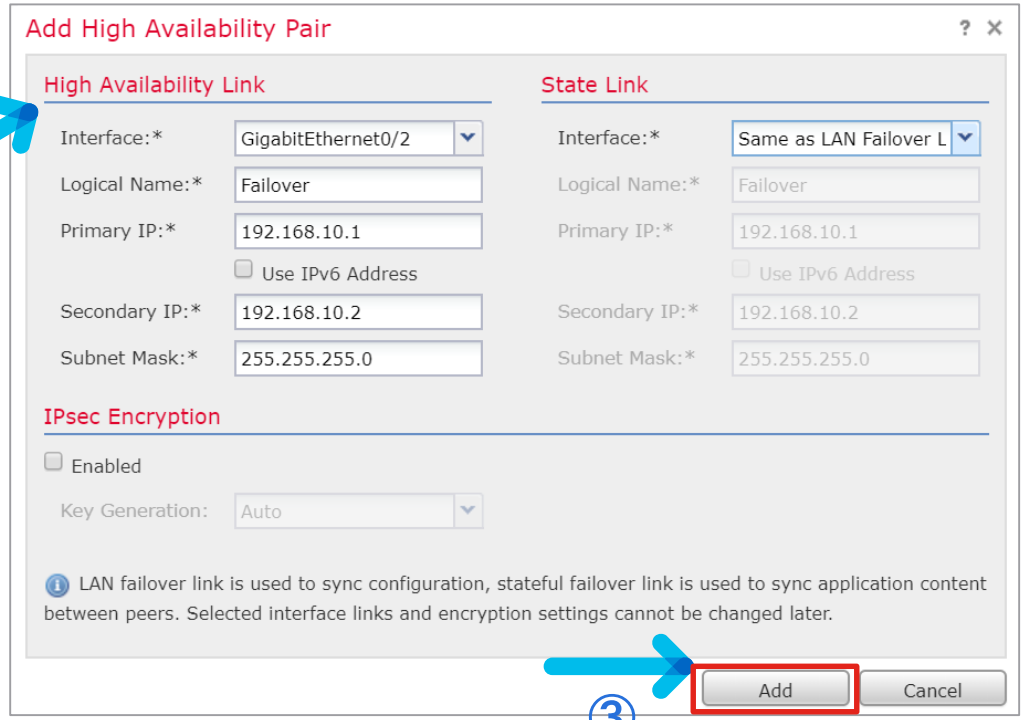
① Device Management > Add > High Availabilityをクリック
② 以下を設定
- Name： FTDv-HA ※任意の名前を記入
- Device Type： Firepower Threat Defenseを選択
- Primary Peer： FTDv01を選択
- Secondary Peer： FTDv02を選択

③ Continueをクリック

ステップ3-1: HA設定 – HAペアの作成(続き)



① HA構成によりSnortプロセスの Restartが発生する警告メッセージが表示。問題なければYesをクリック



① ②

② HAリンク、Stateリンクで以下を設定
HAリンク
- Interface : Gig0/2を選択
- Logical Name: 任意の名前を入力
- Primary IP: FTDv01のHAリンクのIPを入力
- Secondary IP: FTDv02のHAリンクのIP
- Subnet Mask: HAリンクのサブネット

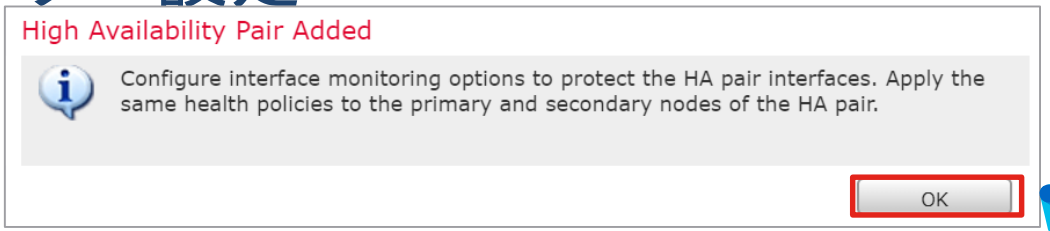
State Link
- Interface: Same as LAN Failover…を選択

③ Addをクリック(クリック後、HA構成開始)

③

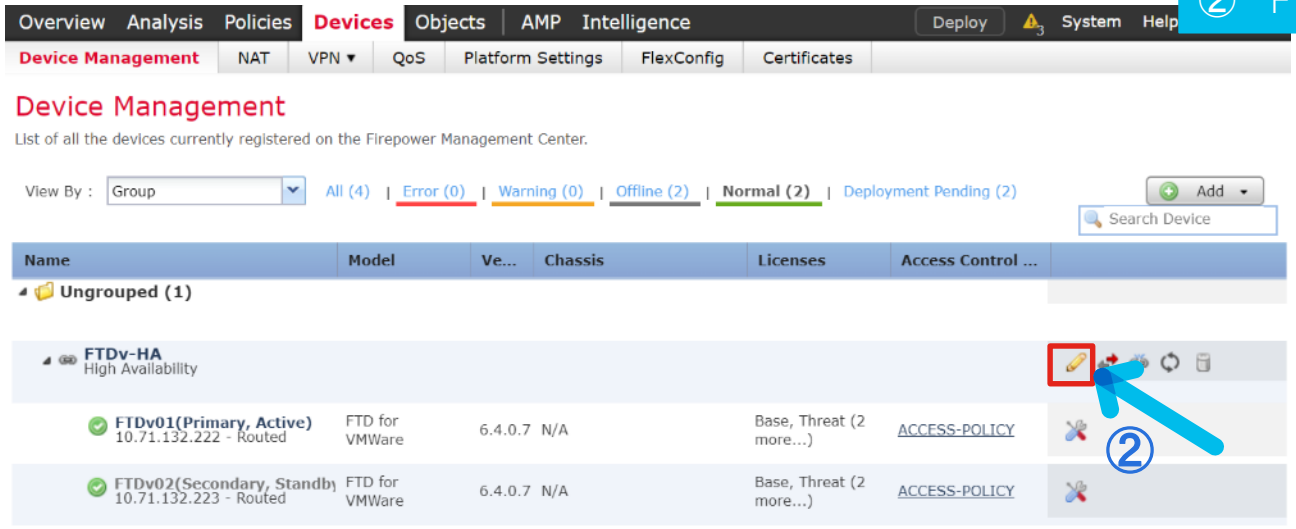
※HA構成完了までに10分以上要する場合もある

ステップ4-1: HA設定 – HAの構成とインタフェースモニター設定

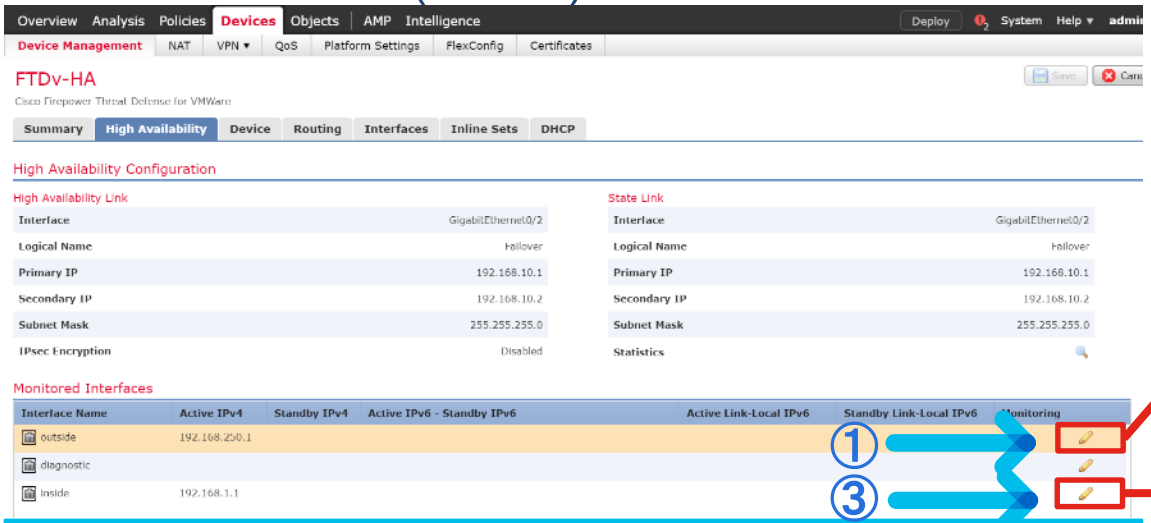


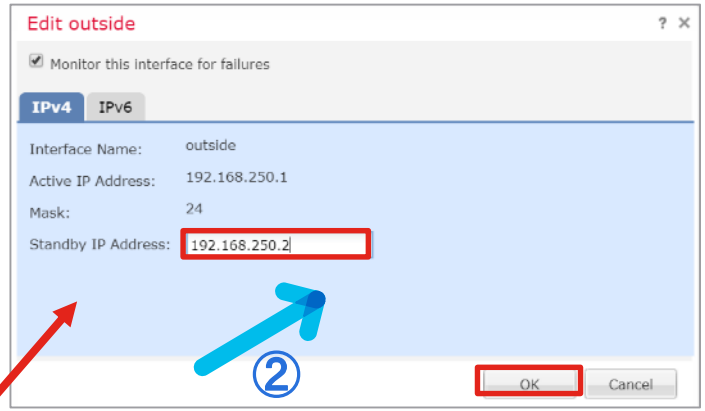
① FTD HAペア登録後のインターフェイスモニター設定や、ヘルスポリシー設定の適用を忘れないように、という情報のポップアップがあるため、OKをクリック

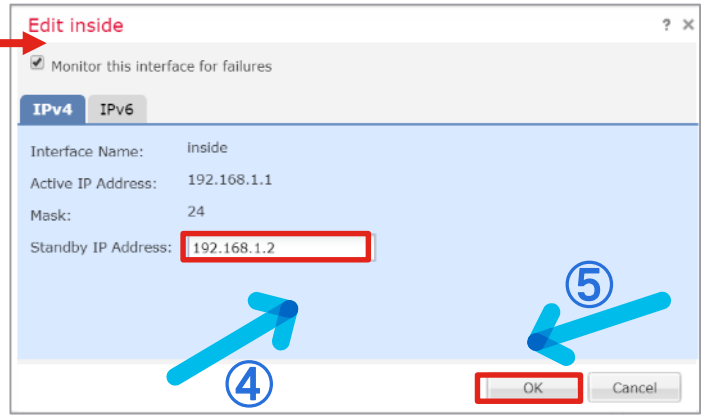
② FTDv-HAの鉛筆マークをクリック



ステップ4-1: HA設定 – HAの構成とインタフェースモニター設定(続き)

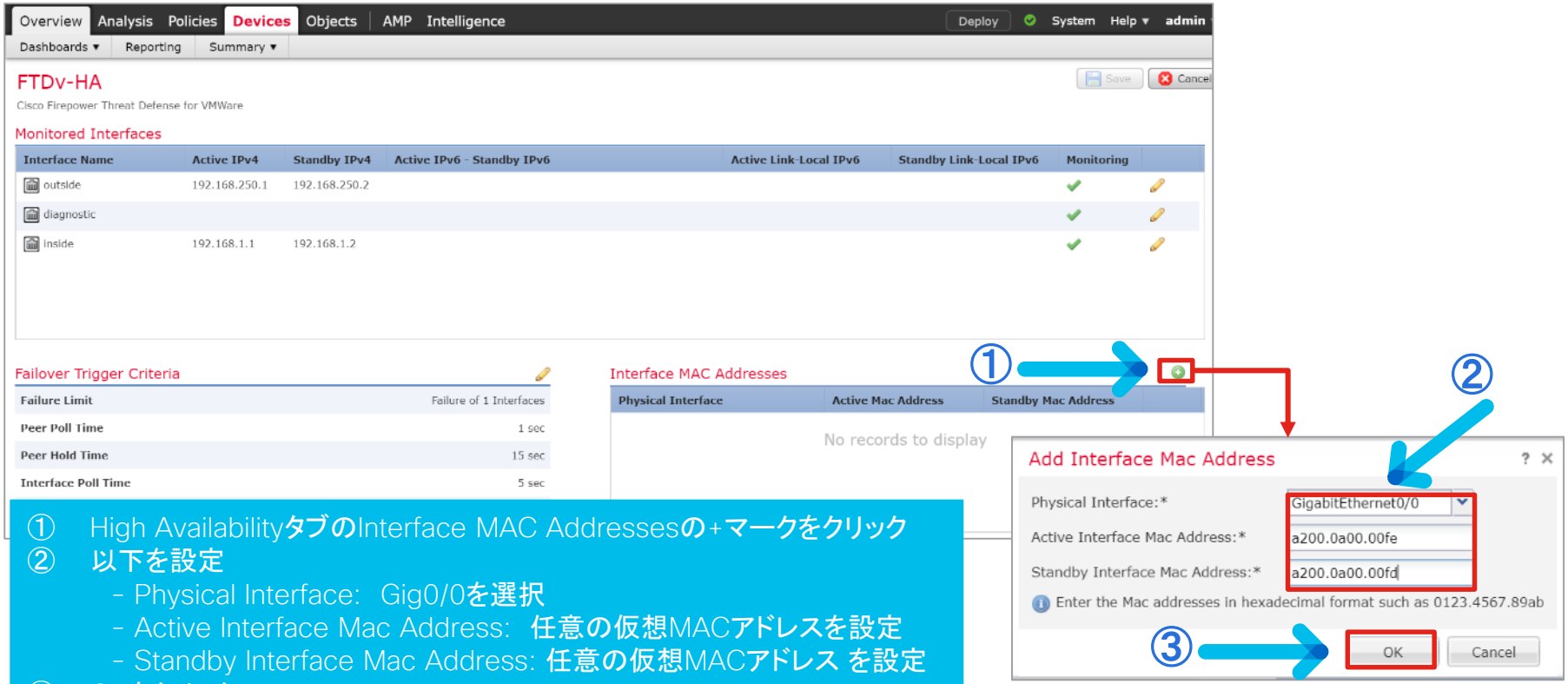






① High Availabilityタブの Monitoring Interfaces > outsideの鉛筆マークをクリック
② Secondary IP AddressにFTDv2のoutside IFモニタ用のIPアドレスを設定し、OKをクリック
③ Insideの鉛筆マークをクリック
④ Secondary IP AddressにFTDv2のinside IFモニタ用のIPアドレスを設定し、OKをクリック
⑤ Saveをクリック

ステップ5-1: HA設定 – 仮想MAC設定

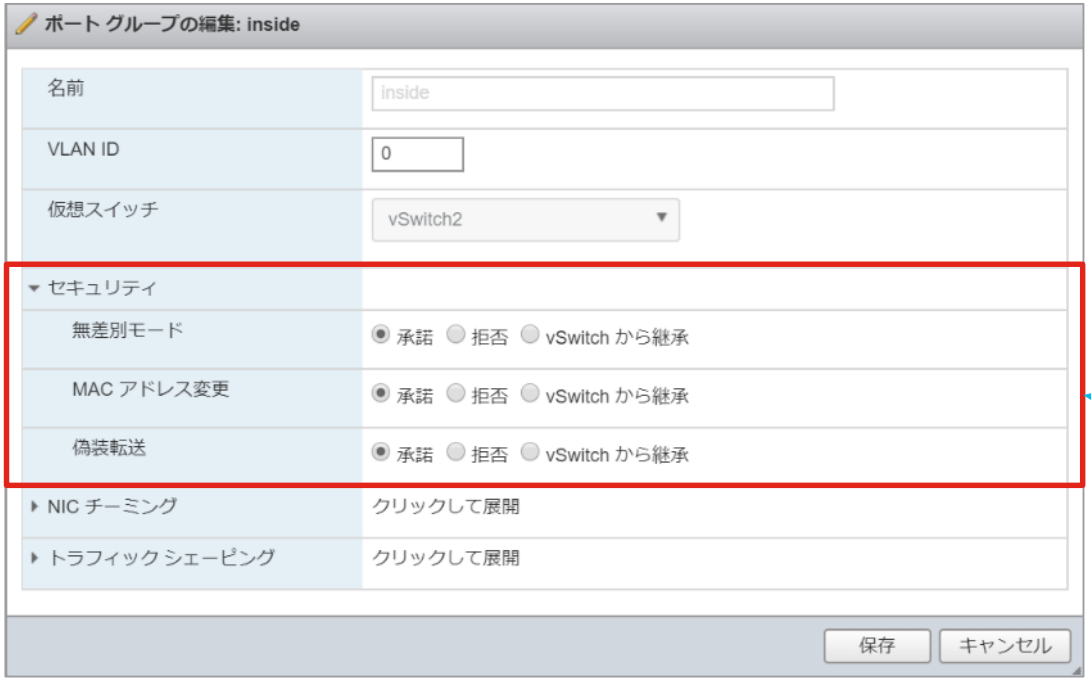


① High Availabilityタブの Interface MAC Addressesの+マークをクリック
② 以下を設定
- Physical Interface: Gig0/0を選択
- Active Interface Mac Address: 任意の仮想MACアドレスを設定
- Standby Interface Mac Address: 任意の仮想MACアドレス を設定

③ OKをクリック
④ 同様にGig0/1でも設定を行い、Saveにて保存

参考：仮想MAC設定におけるvSwitchセキュリティポリシーの設定変更

- VM環境でHAに仮想MACを登録する場合、vSwitchのセキュリティーポリシーの変更が必要となるため注意

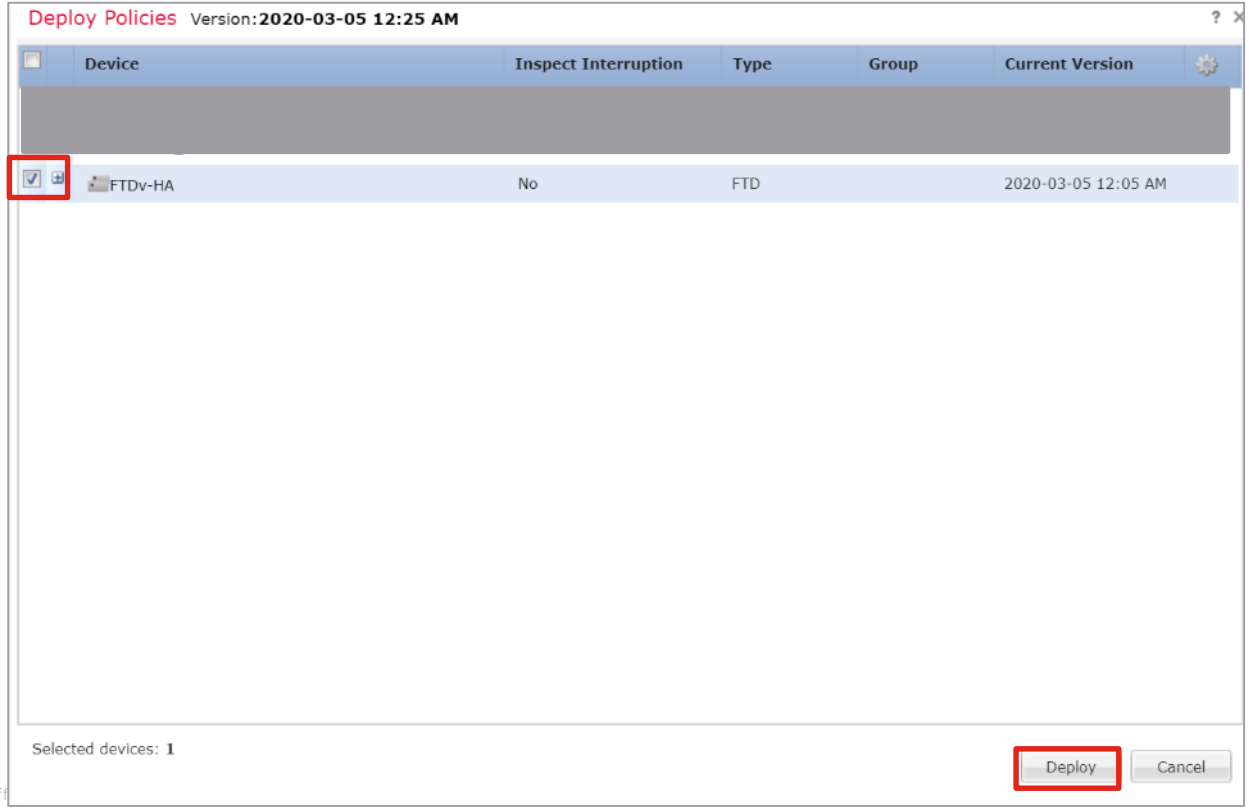


すべて承諾をチェック

https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/vmware/ftdv/ftdv-vmware-qsg.html#24182

ステップ6-1: HA設定 – HAの構成とインタフェースモニター設定

- デプロイの実施



CLIでの確認 – FTDv01へのSSH

```
> show failover
Failover On
Failover unit Primary
Failover LAN Interface: Failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.12(2)151, Mate 9.12(2)151
Serial Number: Ours 9AJU9XP79B5, Mate 9A0KK2GHVAW
Last Failover at: 05:29:44 UTC Mar 30 2020
        This host: Primary - Active
                Active time: 6247 (sec)
                slot 0: ASAv hw/sw rev (/9.12(2)151) status (Up Sys)
                  Interface outside (192.168.250.1): Normal (Monitored)
                  Interface inside (192.168.1.1): Normal (Monitored)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                  Interface outside (192.168.250.2): Normal (Monitored)
                  Interface inside (192.168.1.2): Normal (Monitored)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)

Stateful Failover Logical Update Statistics
        Link : Failover GigabitEthernet0/2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         902        0          830        0
        sys cmd         830        0          830        0
        up time         0          0          0          0

……..以下省略
```

HAリンクがUP状態

Primary機の状態

モニタ対象のIFの状態（Normal）

モニタ対象のSnortとDiskの状態（Up）

Secondary機の状態

モニタ対象IFの状態（Normal）

モニタ対象のSnortとDiskの状態（Up）

Stateリンクが UP状態

CLIでの確認 – FTDv01へのSSH

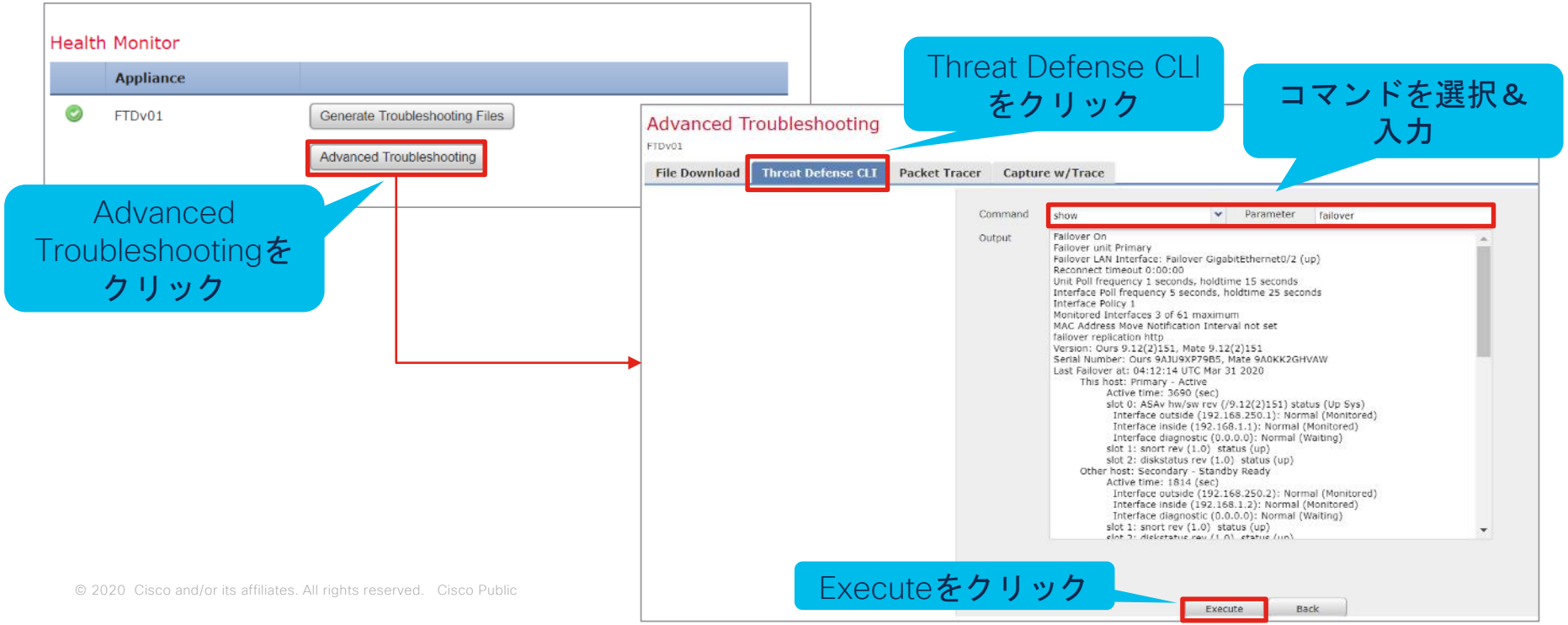
- show failover historyコマンドで、障害検知などによるActive機とStandby機の切り替え(failover)理由の確認可能
- Primary機(FTDv01)より実施

```
> show failover history
==========================================================================
From State               To State               Reason
==========================================================================
....省略
05:29:44 UTC Mar 30 2020
Active Config Applied    Active                 No Active unit found

07:37:04 UTC Mar 30 2020
Active                   Failed                 Interface check
                                                This host:1
                                                single_vf: outside
                                                Other host:0

==========================================================================
```

モニタ対象のIFのリングダウンを検知

参考：FMCでのHAステータス確認

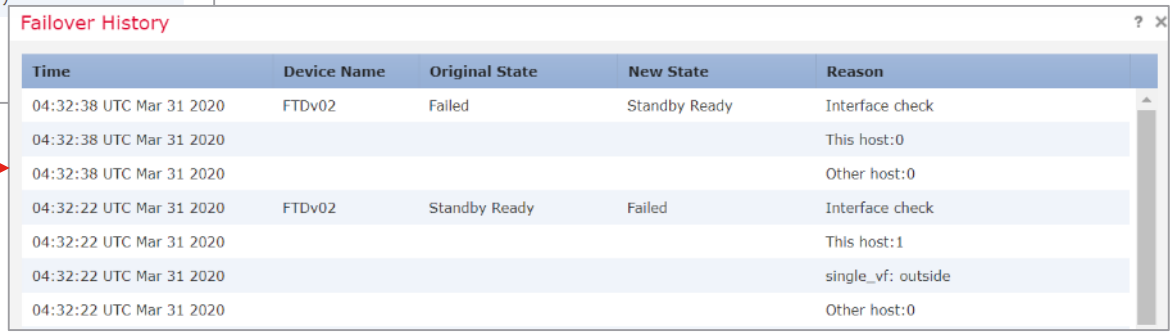
- show failoverをFMCから確認する方法
- Health > Monitor > 対象のFTDデバイスをクリック



参考：FMCでのHAステータス確認

- failover historyもFMCより確認可能
- Device > Device Management > HAの鉛筆マーク > Summary

虫眼鏡アイコンを
クリック



HA Active機の切り替え

- Devices > Device Managementより
- Primary機障害時の切り戻し等での利用

HAの解除

- Devices > Device Managementより
- HA構成を解除して単体のFTDに戻す場合に利用

HAのベストプラクティス

- 以下のFTD HA ベストプラクティスにそって導入することで、トラブル発生リスクを抑えることが可能
  - FTD HAのデータインターフェイスは、スイッチ もしくは HUBでの収容が推奨。
  - スイッチを利用時は、Portfast もしくは 同等の設定を スイッチ側ポートで有効化すること。冗長構成 障害時の素早い通信再開や、インターフェイスアップ後のGARP送付に必要
  - FTD HAの High Availability Link (=Failover Link) と State Linkは、FTDデバイス間で直結、もしくは EtherChannelを利用。特に通信量の多い環境の場合、多量の同期情報が当Link内を流れるため、広帯域のインターフェイスを利用すること
  - データインターフェイスには、Active IPアドレスと Standby IPアドレスを両方設定することが推奨。2つのIPアドレスを設定することで、両ポート間の動的監視が可能に
  - (特にNAT利用時は) データインターフェイスには、Active 仮想MACアドレスと Standby 仮想MACアドレスの設定が推奨。仮想MACアドレスを設定することで、保守交換時のMACアドレス変動や それに伴う通信影響を抑えることができる。
  - Interface監視のための Polltimeや Holdtimeは デフォルト値利用が推奨。短すぎるPolltimeや Holdtimeは、過剰な通信や負荷が発生時の 短時間のHelloパケットのドロップによる、予期せぬ切り替えの発生原因に。

Firepower System: FTD HA: FTD冗長構成の組み方とトラブルシューティング (FMC利用時)
https://community.cisco.com/t5/-/-/ta-p/3952716

Appendix
1. マルチインスタンスの作成

マルチインスタンスの概要

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

参考：各製品で作成可能なFTDインスタンス数

・2つの制限の小さい方
(CPUコア数/ディスク容量)

CPUコアは1インスタンスにつき最低6コア必要

ディスク容量は1インスタンスにつき最低48GB必要

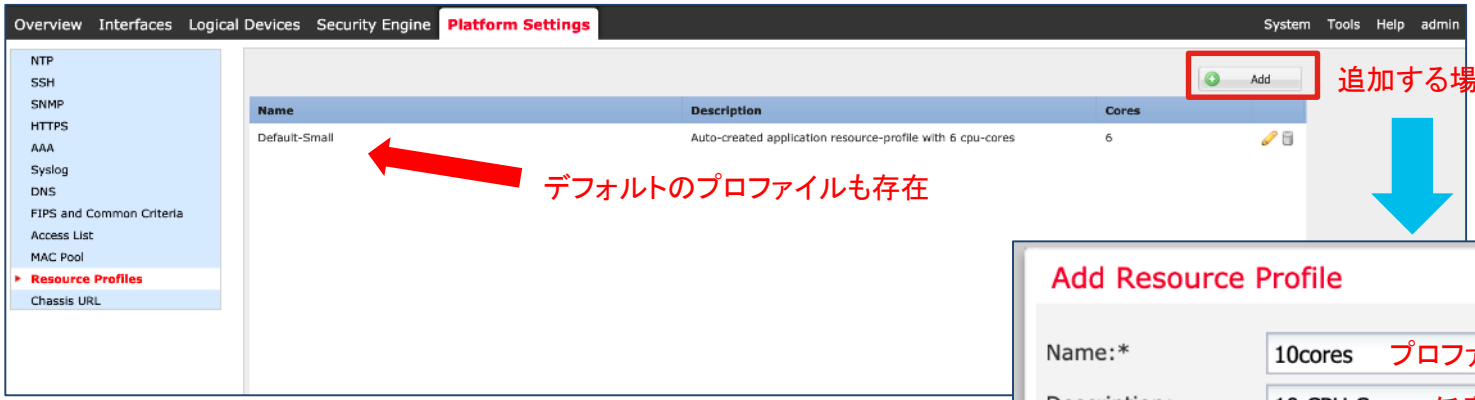
プラットフォーム	CPUコア保持数	デフォルトのCPUコア割り当て (Data Plane/Snort/System)	トータルアプリディスク容量	最大FTDインスタンス	
				CPU Bound	Disk Bound
Firepower 4110	22	8/12/2	150Gb	3	~~3~~
Firepower 4115 new	46	16/28/2	350Gb	7	~~7~~
Firepower 4120	46	20/24/2	150Gb	~~7~~	3
Firepower 4125 new	62	24/36/2	750Gb	10	~~15~~
Firepower 4140	70	32/36/2	350Gb	~~11~~	7
Firepower 4145 new	86	32/52/2	750Gb	14	~~15~~
Firepower 4150	86	36/48/2	350Gb	~~14~~	7
Firepower 9300 SM-24	46	20/24/2	750Gb	7	~~15~~
Firepower 9300 SM-36	70	32/36/2	750Gb	11	~~15~~
Firepower 9300 SM-40 new	78	32/44/2	1.55Tb	13	~~32~~
Firepower 9300 SM-44	86	36/48/2	750Gb	14	~~15~~
Firepower 9300 SM-48 new	94	40/52/2	1.55TB	15	~~32~~
Firepower 9300 SM-56 new	110	44/64/2	1.55TB	18	~~32~~

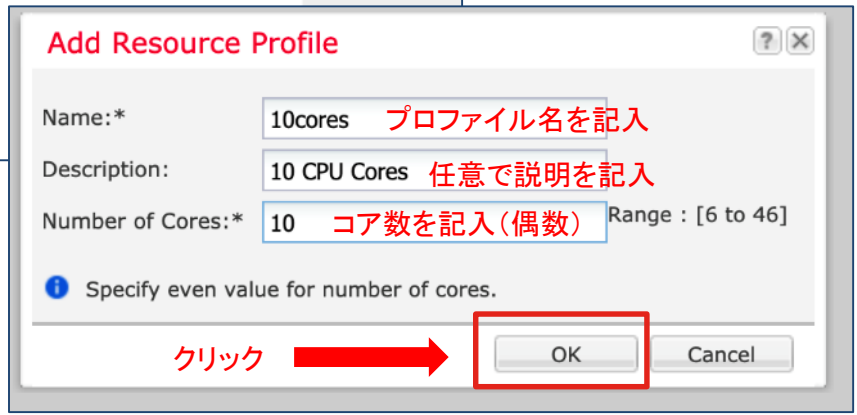
ステップ 1-1: マルチインスタンス用プロファイル作成

■FCM(Firepower Chassis Manager)へログイン後 Platform Settings > Resource Profiles

※FMCではなく通常のインスタンス作成と同じようにFCMの画面で設定を行う

FTDインスタンスを複数作成するために必要なResource Profilesの確認と作成。

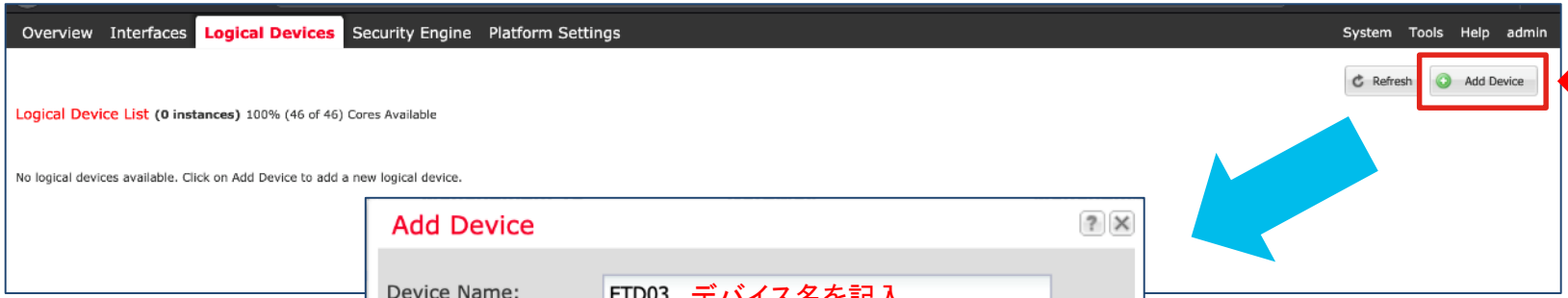




ステップ 1-2: マルチインスタンス作成

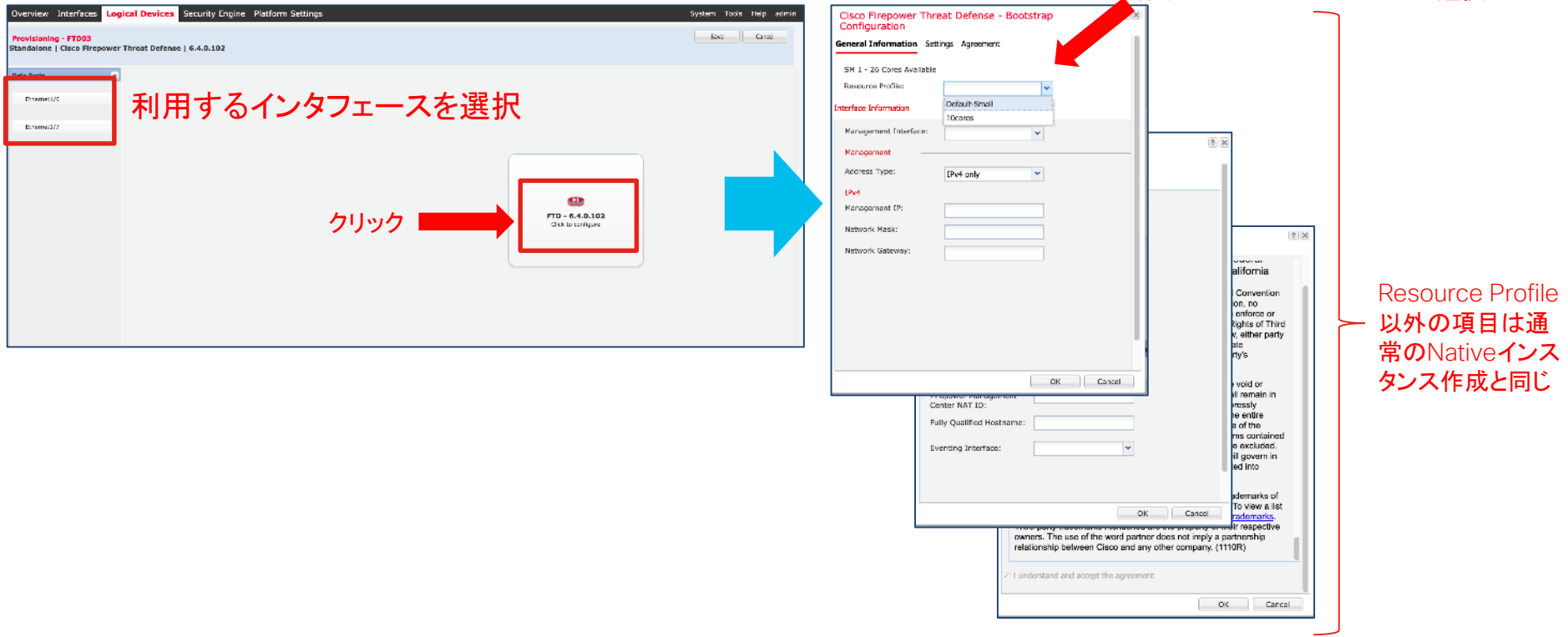
※Nativeで作成した場合のCPUコア割り当ては参考ページの表に記載

Logical Devices > Add Device



※マルチインスタンスの場合は
必ずContainerを選択
Nativeを選ぶとすべてのリソースが1台のインスタンスに割り当たるためあとから追加で複数のインスタンスを構築するのは不可となる。

ステップ 1-3: マルチインスタンス作成



参考：FTDインスタンス複数作成後の状態

Appendix
2. FMCアプライアンスHA構成のアップグレード方法

FMC2500 HAペアイメージアップグレード概要

- アップグレード対象
  - 本資料ではFMC2500 HAペア v6.3.0.3から v6.4.0.7を対象
- HAペアの場合、全てのアップグレード手順はStandby機(通常Secondary)から行う

FMC2500 HAペアイメージアップグレード

- アップグレードステップ
  1. 6.4.0および6.4.0.7のイメージをダウンロード
  2. イメージをPrimary/Secondary FMCへアップロード
  3. 未Deployの設定がないかを確認
  4. HAの同期停止(Pause Synchronization)
  5. Secondary FMCのアップグレード(6.3.0.3 → 6.4.0 → 6.4.0.7)
  6. Primary FMCのアップグレード(6.3.0.3 → 6.4.0 → 6.4.0.7)
  7. (オプション/推奨)Hotfixの適用
  8. HAの同期を再開

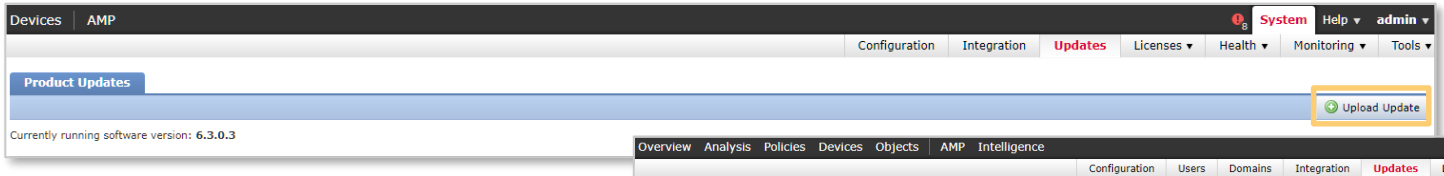
1. アップグレードイメージのダウンロード

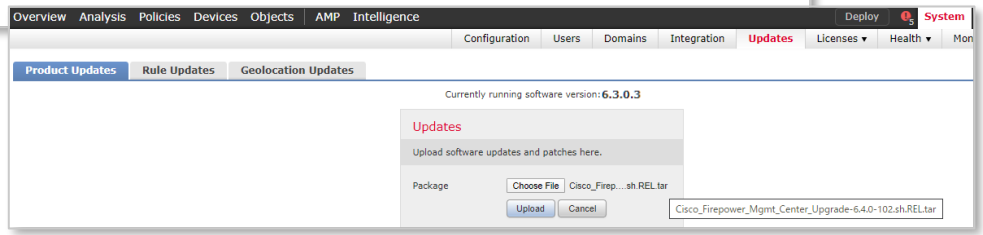
- v6.3.0.3からのアップグレードの場合、まずはv6.4.0を適用
  - ソフトウェアセンターよりイメージをダウンロード
    v6.4.0
    Cisco_Firepower_Mgmt_Center_Upgrade-6.4.0-102.sh.REL.tar
    v6.4.0.7
    Cisco_Firepower_Mgmt_Center_Patch-6.4.0.7-53.sh.REL.tar
    Hotfix (BIOS Update)
    Cisco_Firepower_Mgmt_Center_BIOSUPDATE_640_CJ-12.sh.REL.tar

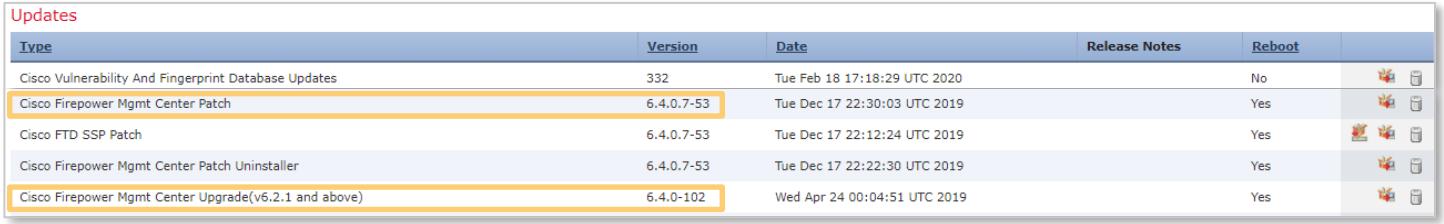
    Release Note:
    https://www.cisco.com/c/en/us/support/security/defense-center/products-release-notes-list.html

2. アップグレードイメージをFMCへアップロード

- Primary/Secondary FMCへアップグレードイメージのアップロード
  - System > Updates > Upload Update よりイメージをアップロード



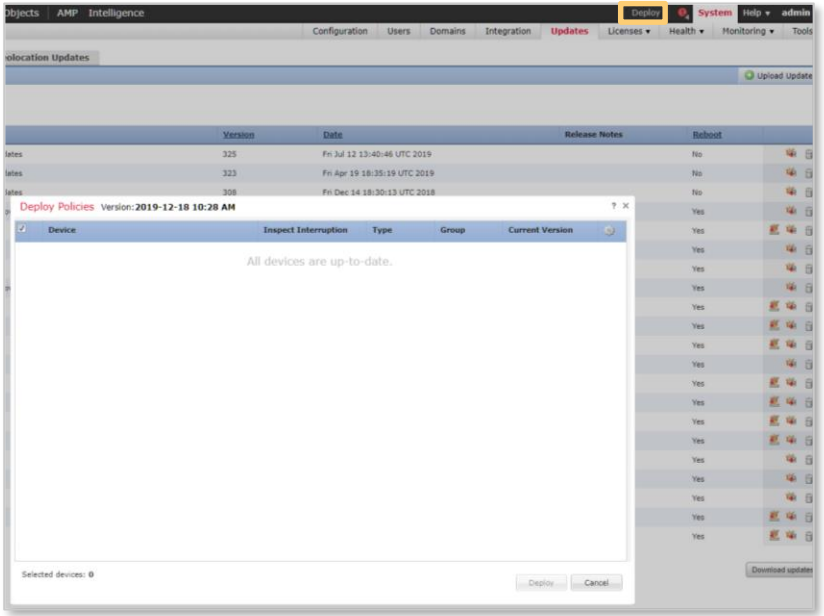




※インターネットアクセスがある場合、Download Updatesボタンで最新のイメージをCCOからダウンロードする事も可

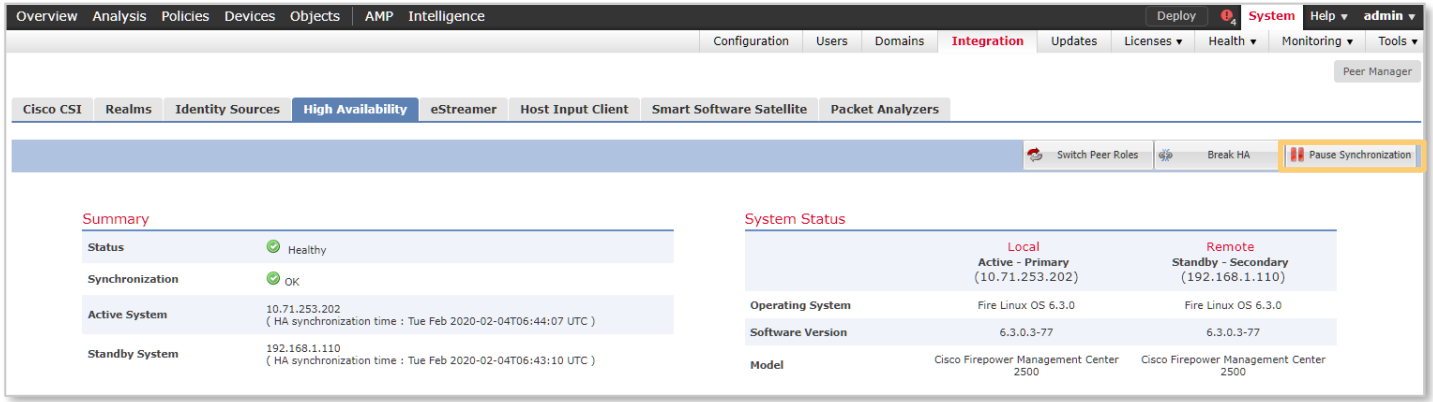
3. 未Deployの設定がないかを確認

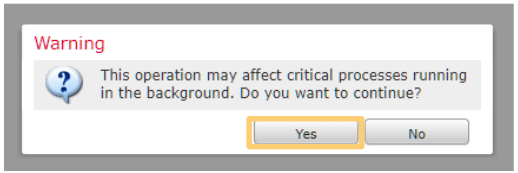
- Deployボタンにて Deploy待ちのデバイスや、その他エラーなどないかを確認(FMCがヘルシーな状態であるかを確認)

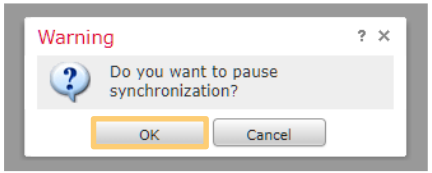


4. HAの同期停止

- Primary FMCにて一時的に同期の停止
  - System > Integration > High Availability > Pause Synchronization

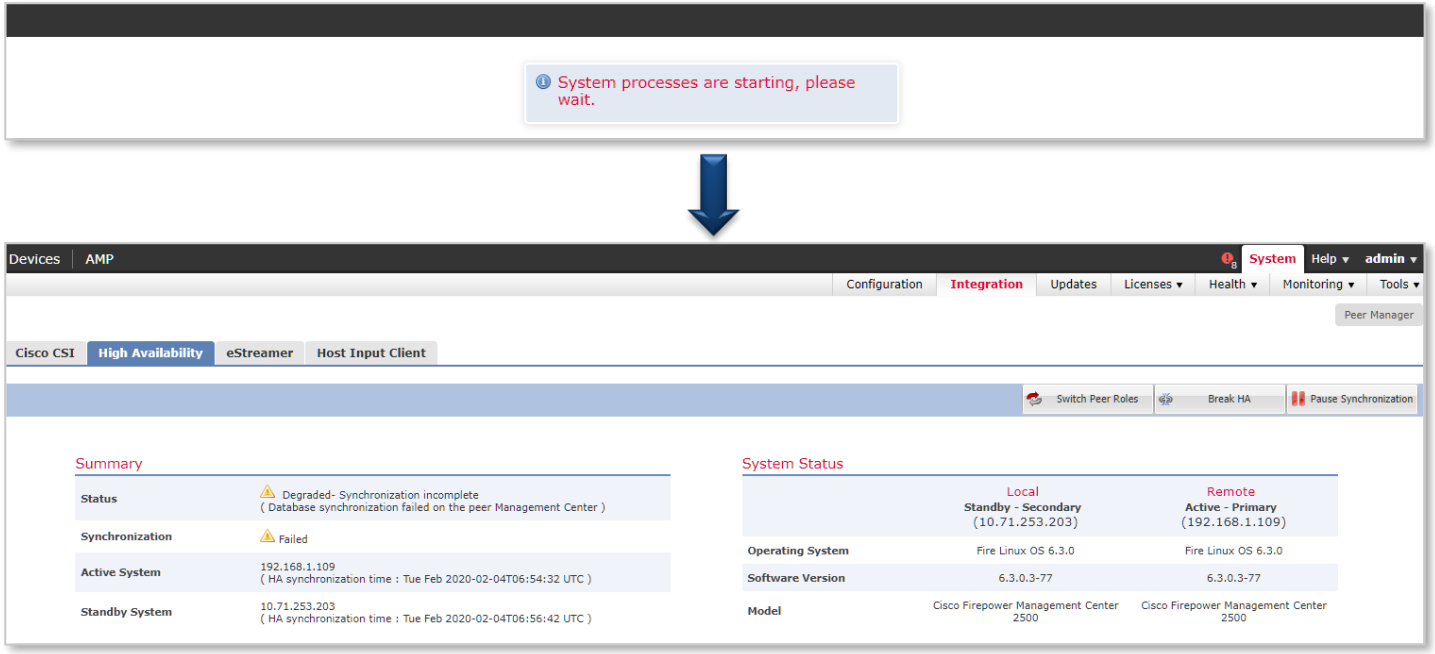






※WarningにはYes/OKをクリック

4. HAの同期停止

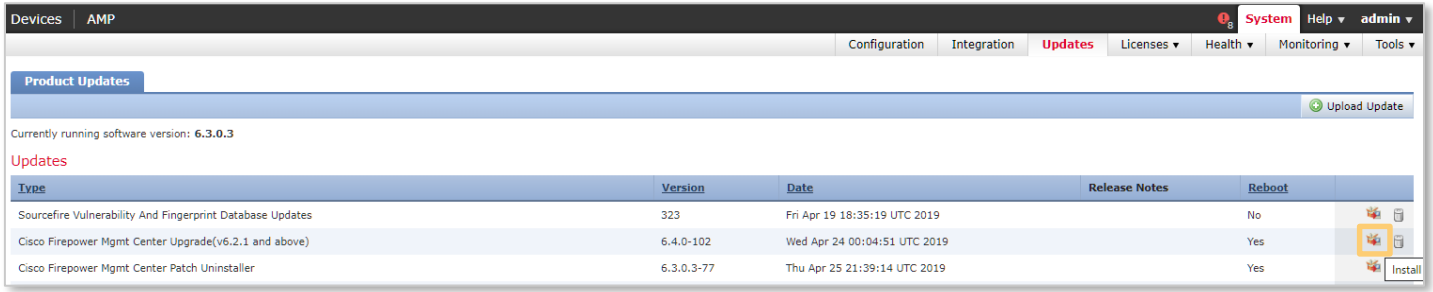


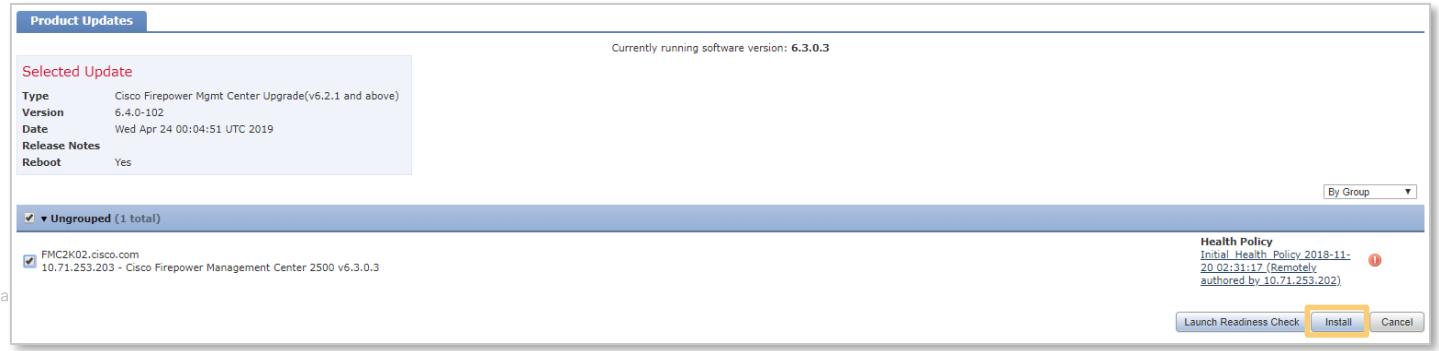
※Secondary側

5. Secondary FMCのアップグレード

v6.3.0.3 → v6.4.0

- Standby機であるSecondaryよりアップグレードを開始
- System > Updates より該当のイメージを選択しInstallをクリック



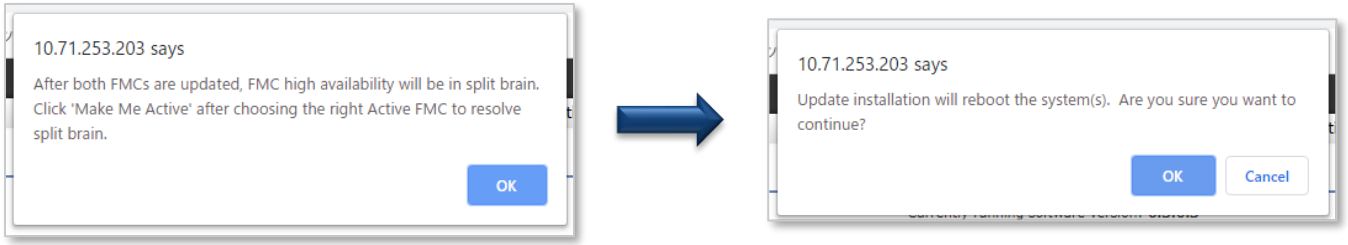


※Health Alertはラボ環境により電源モジュール2に電源が入っていないため

5. Secondary FMCのアップグレード 2/4

v6.3.0.3 → v6.4.0

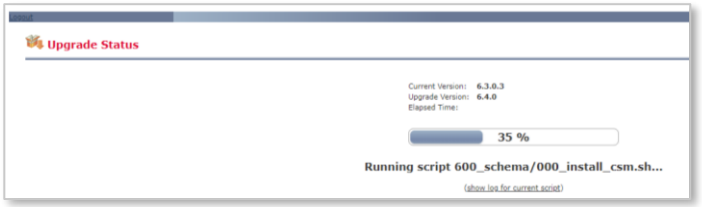
- Installボタンを押した後、アップグレード後にSplit Brain 状態となるWarningメッセージが表示

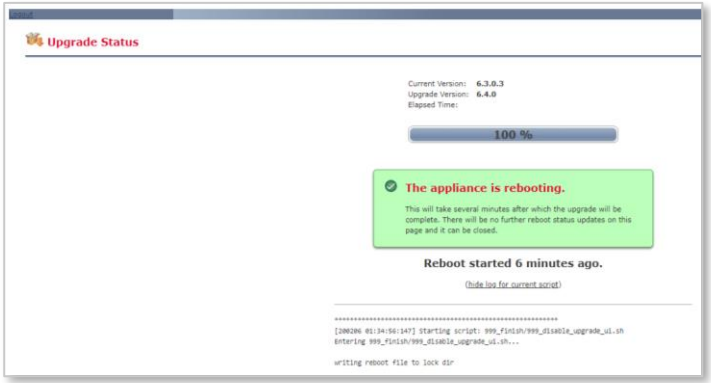


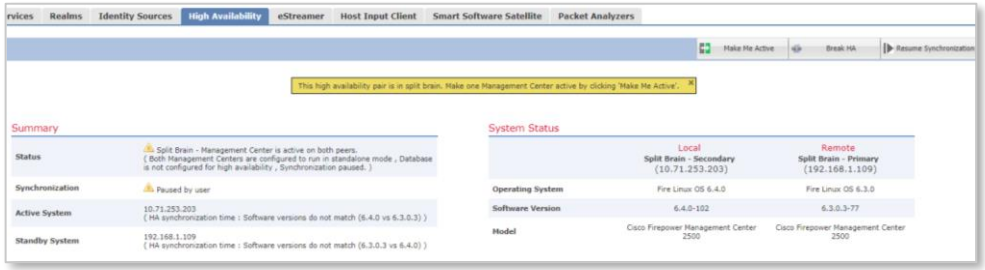
5. Secondary FMCのアップグレード 3/4

v6.3.0.3 → v6.4.0

・イメージアップグレード後、FMCはリブートしアップグレード終了





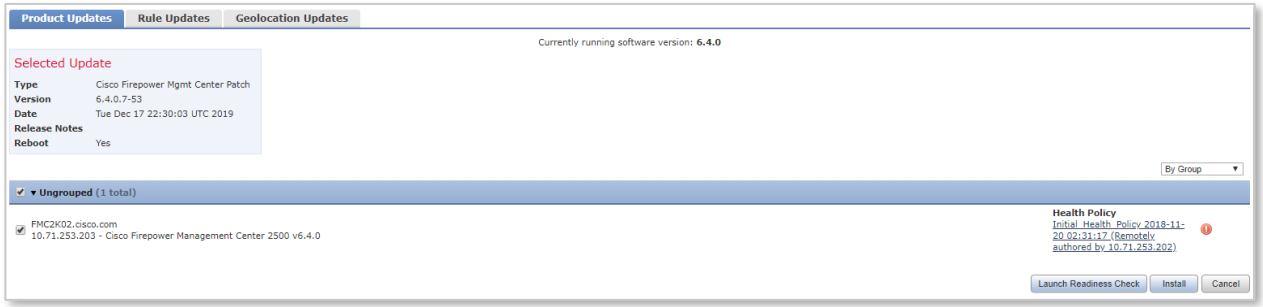


※Upgrade後、HAの状態はSplit Brainとなる

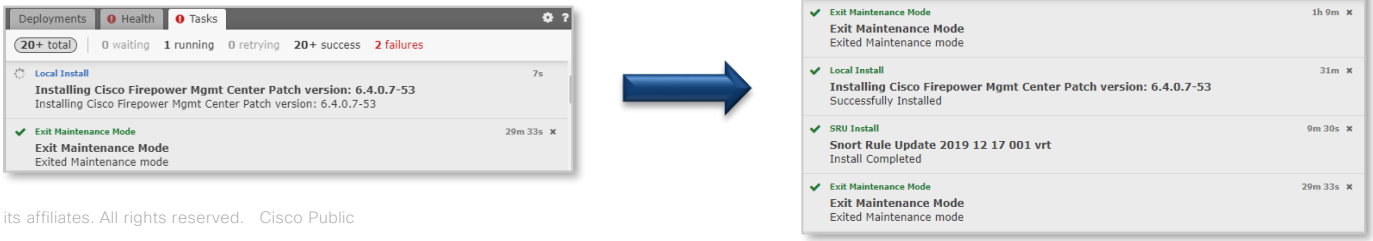
5. Secondary FMCのアップグレード

v6.4.0 → v6.4.0.7

- System > Updates より該当のイメージを選択しInstallをクリック



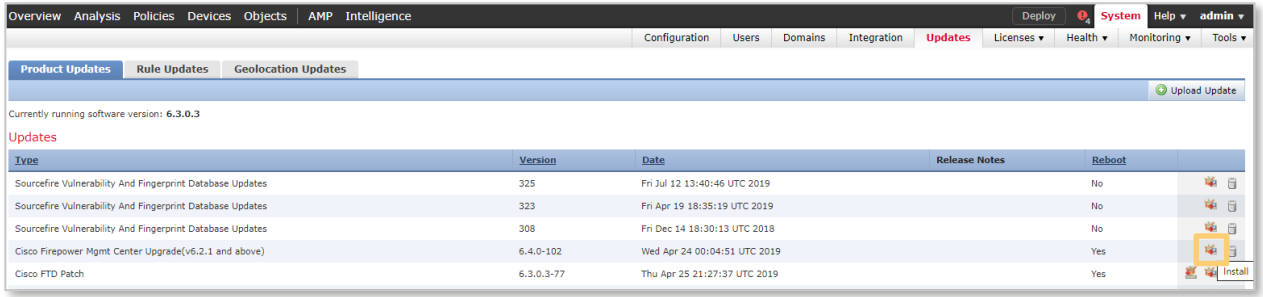
- アップグレード状況はTasksでも確認可

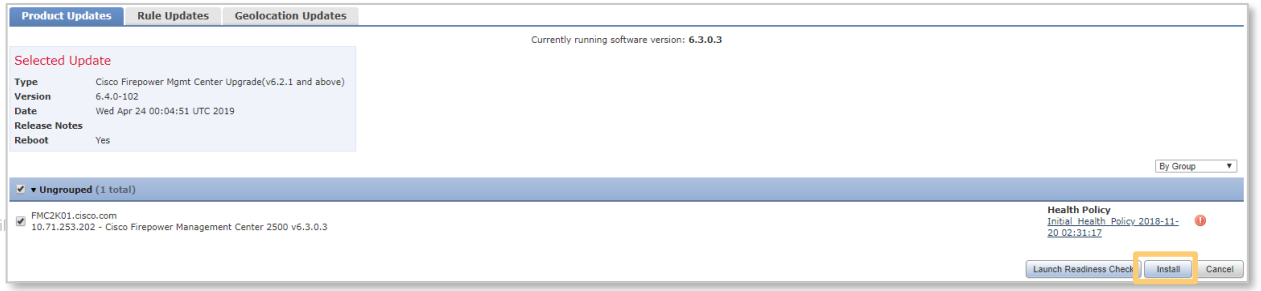


6. Primary FMCのアップグレード

v6.3.0.3 → v6.4.0

- Standby機のアップグレード終了後、Active機であるPrimaryのアップグレードを開始
- System > Updates より該当のイメージを選択しInstallをクリック



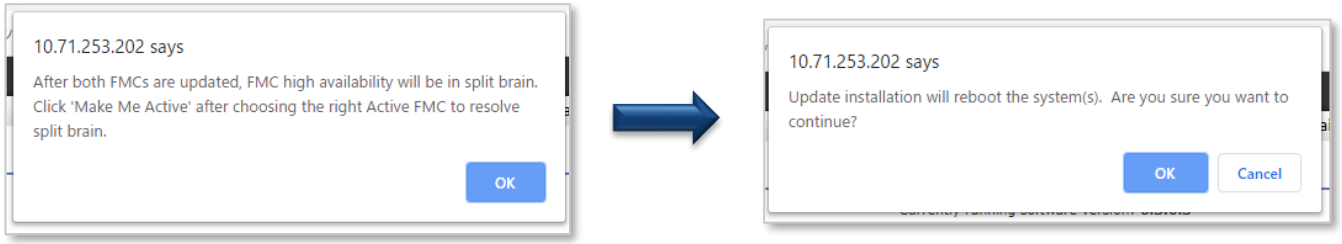


※Health Alertはラボ環境により電源モジュール2に電源が入っていないため

6. Primary FMCのアップグレード

v6.3.0.3 → v6.4.0

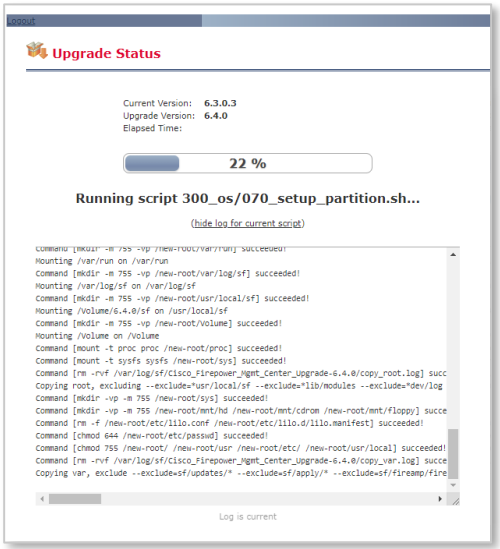
- Installボタンを押した後、アップグレード後にSplit Brain 状態となるWarningメッセージが表示

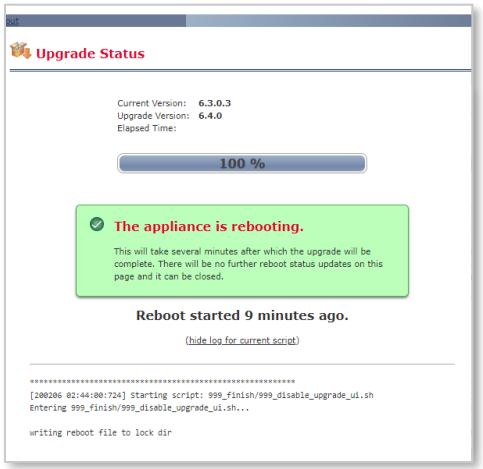


6. Primary FMCのアップグレード

v6.3.0.3 → v6.4.0

・イメージアップグレード後、FMCはリブートしアップグレード終了

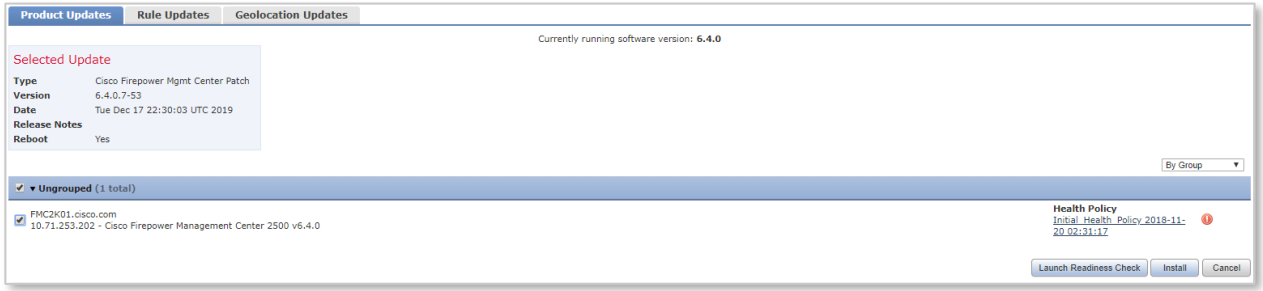




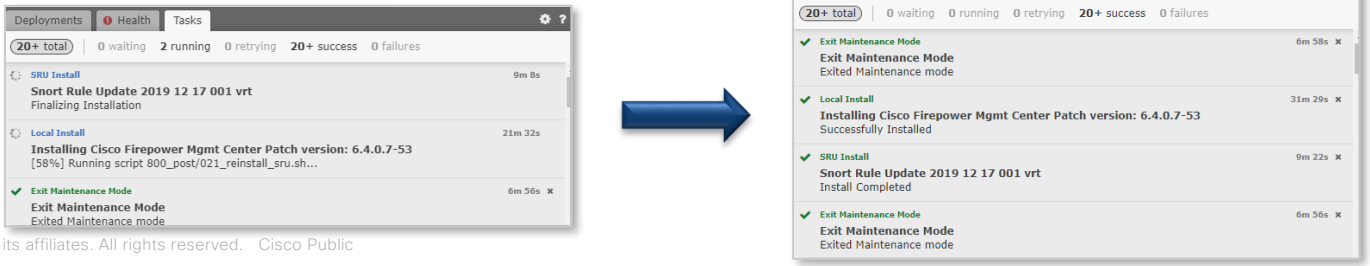
6. Primary FMCのアップグレード

v6.4.0 → v6.4.0.7

- System > Updates より該当のイメージを選択しInstallをクリック



- アップグレード状況はTasksでも確認可



7. Hotfixの適用

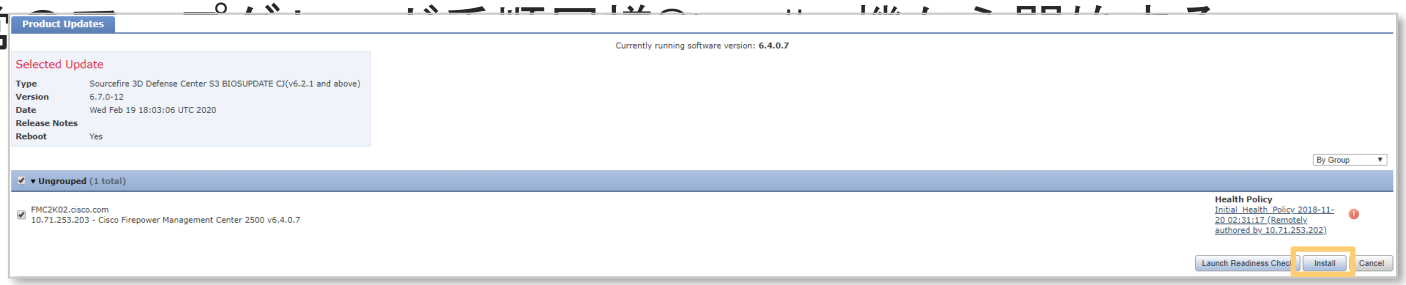
- 最新のHotfixの適用(Hotfix CJにはBIOSアップデートが含まれる)
- 両FMCコンソールにてBIOSの確認(`sudo dmidecode -t bios -q`)

```
admin@FMC2K02:~$ sudo dmidecode -t bios -q
Password:
BIOS Information
        Vendor: Cisco Systems, Inc. FMC5
        Version: C220M4.2.0.13d.0.0812161113
        Release Date: 08/12/2016
<snip>
        BIOS Revision: 5.11
```

```
admin@FMC2K01:~$ sudo dmidecode -t bios -q
Password:
BIOS Information
        Vendor: Cisco Systems, Inc. FMC5
        Version: C220M4.2.0.13d.0.0812161113
        Release Date: 08/12/2016
<snip>
        BIOS Revision: 5.11
```

※2.0.13dが現時点のバージョン

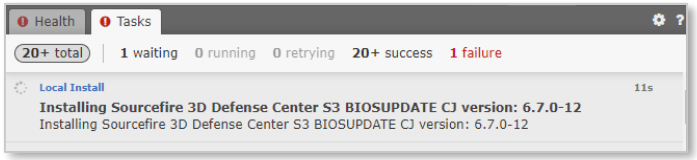
- 通常



7. Hotfixの適用

- インストール後、FMCはリブートしBIOSのアップデートが完了

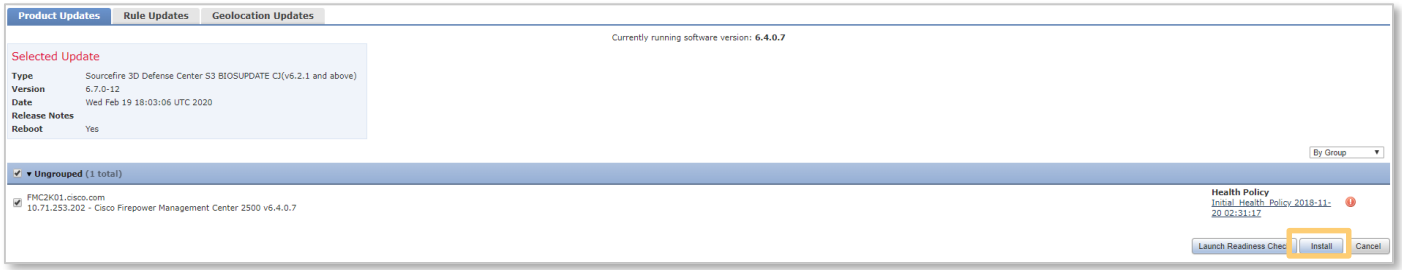
Standby FMC GUI



Standby FMC コンソール

```
admin@FMC2K02:~$ sudo dmidecode -t bios -q
Password:
BIOS Information
      Vendor: Cisco Systems, Inc., FMC
      Version: C220M4.4.0.2d.0.0627191019
      Release Date: 06/27/2019
<snip>
      BIOS Revision: 5.11
```

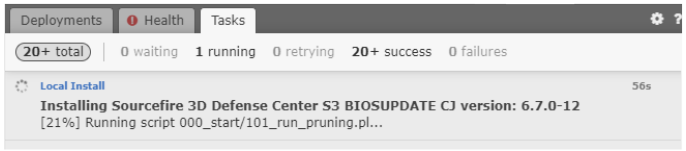
- Active機へのHotfix適用



7. Hotfixの適用

・インストール後、FMCはリブートしBIOSのアップデートが完了

Active FMC GUI

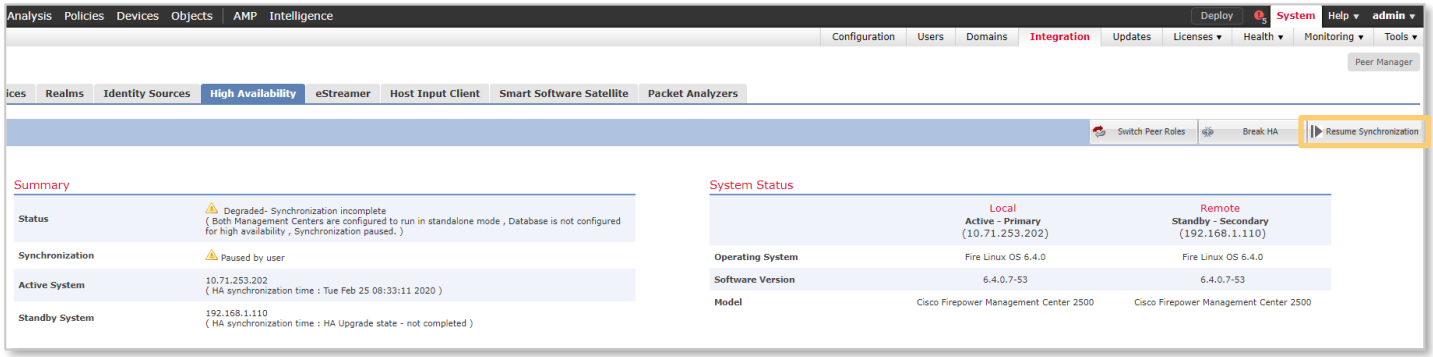


Active FMC コンソール

```
admin@FMC2K01:~$ sudo dmidecode -t bios -q
Password:
BIOS Information
      Vendor: Cisco Systems, Inc., FMC
      Version: C220M4.4.0.2d.0.0627191019
      Release Date: 06/27/2019
<snip>
      BIOS Revision: 5.11
```

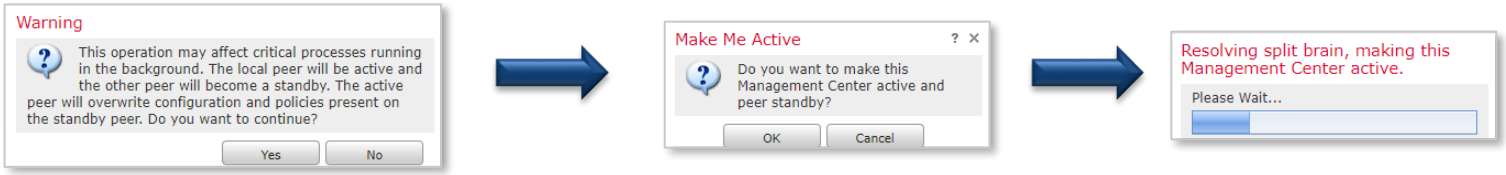
8. HAの同期再開

- Primary/Secondaryにてアップグレード完了後、HAの同期を再開する
- HAの同期再開は、Active機として動作させたい機器(通常Primary)にて操作する
- System > Integration > High Availability にて Resume Synchronizationをクリック

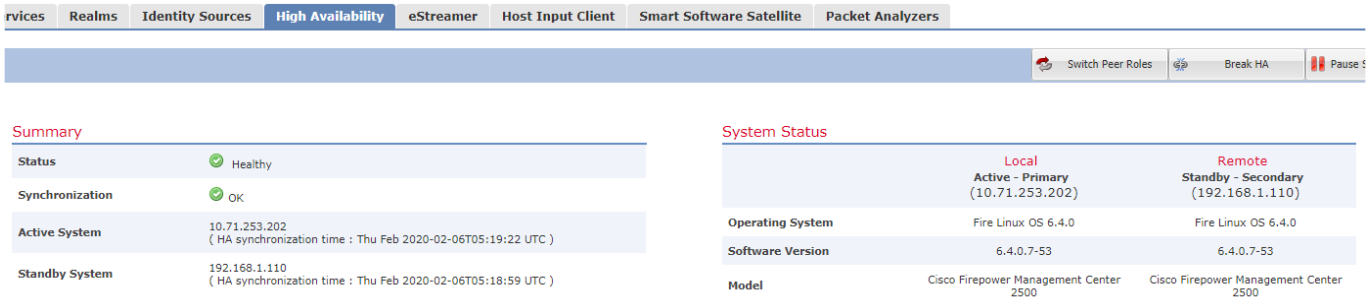


8. HAの同期再開 2/2

- 同期開始前にWarningが送信されるため、Yes/OKで同期を開始する



- 同期終了後、StatusがHealthyかつSynchronizationがOKなことを確認



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
- [重要] 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