



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

Management

.132.222

G0/0 outside .1

FTDv01

G0/1 inside .1

.132.221

FMCv

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

g0/0 グローバルアドレス

ASA

g0/2 .254

外部LAN
192.168.250.0/24

Switch

#g1/0/1
#g1/0/2

PAT

PAT

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。

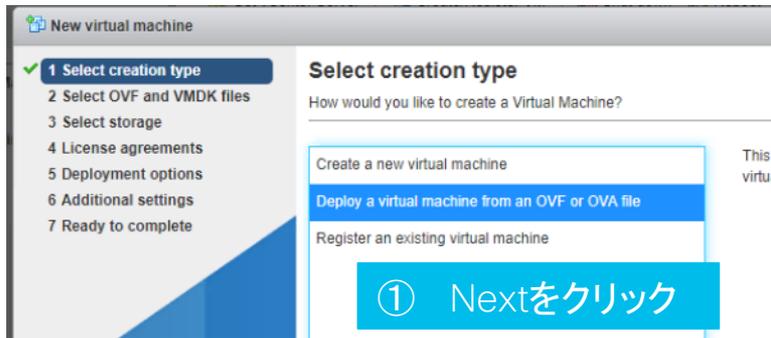
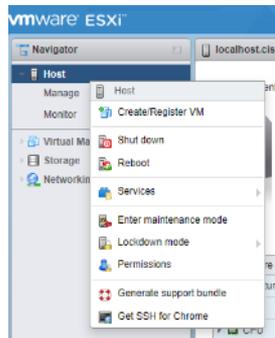
FMCv: VMware install package for ESXi 6.0 and 6.5
Cisco_Firepower_Mgmt_Center_Virtual_VMware-6.4.0-102.tar.gz

24-Apr-2019

2210.28 MB



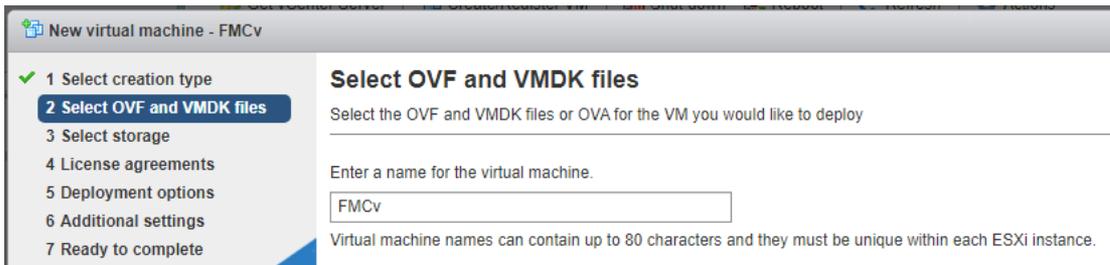
3. vSphere Clientで展開したOVFをデプロイしていく





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

Click to select files or drag/drop

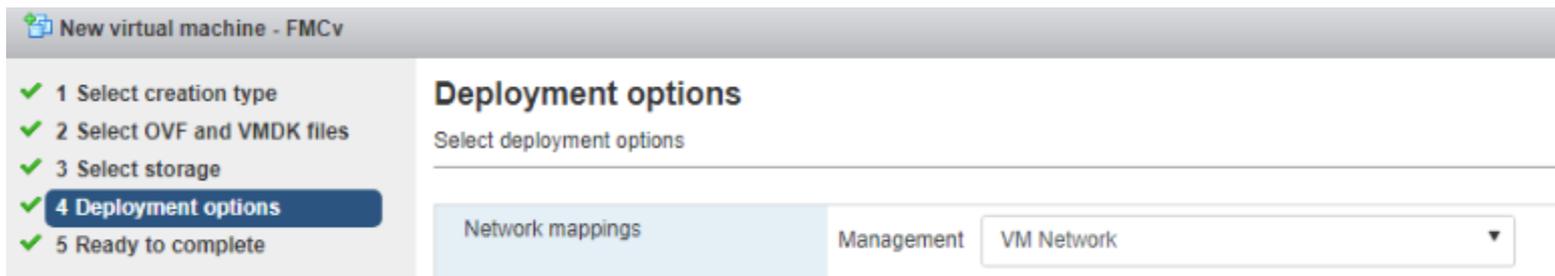
- ☐ Cisco_Firepower_Mgmt_Center_Virtual_VMware-6.4.0-102-disk1.vmdk
- ☐ Cisco_Firepower_Mgmt_Center_Virtual_VMware-ESXi-6.4.0-102.mf
- ☑ Cisco_Firepower_Mgmt_Center_Virtual_VMware-ESXi-6.4.0-102.ovf
- ☐ Cisco_Firepower_Mgmt_Center_Virtual_VMware-VI-6.4.0-102.mf
- ☐ Cisco_Firepower_Mgmt_Center_Virtual_VMware-VI-6.4.0-102.ovf

- × Cisco_Firepower_Mgmt_Center_Virtual_VMware-ESXi-6.4.0-102.ovf
- × Cisco_Firepower_Mgmt_Center_Virtual_VMware-6.4.0-102-disk1.vmdk



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



Change Password

Use these fields to change the password for the admin account. Cisco recommends that you use a password that has at least 8 characters, including uppercase and lowercase letters, numbers, and special characters. Avoid using words that appear in a dictionary.

New Password ①

Confirm

Network Settings

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

Protocol IPv4 IPv6 Both

IPv4 Management IP ②

Netmask

IPv4 Default Network Gateway

Hostname

Domain

Primary DNS Server

Secondary DNS Server

Tertiary DNS Server

Time Settings

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

Set My Clock ③

Via NTP from

Manually

2020 / January / 20 / 19 : 14

Current Time 2020-01-21 09:22

Set Display Time Zone Asia/Tokyo

Recurring Rule Update Imports

Use these fields to schedule recurring rule updates.

Install New

Enable Recurring Rule Update Imports from the Support Site

Import Frequency Daily at 9:00 PM Asia/Tokyo

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

Recurring Geolocation Updates

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

Install New

Enable Recurring Weekly Updates from the Support Site

Update Start Time Sunday 06:00 PM Asia/Tokyo ④

End User License Agreement

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

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

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

Apply

- 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

⑤

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



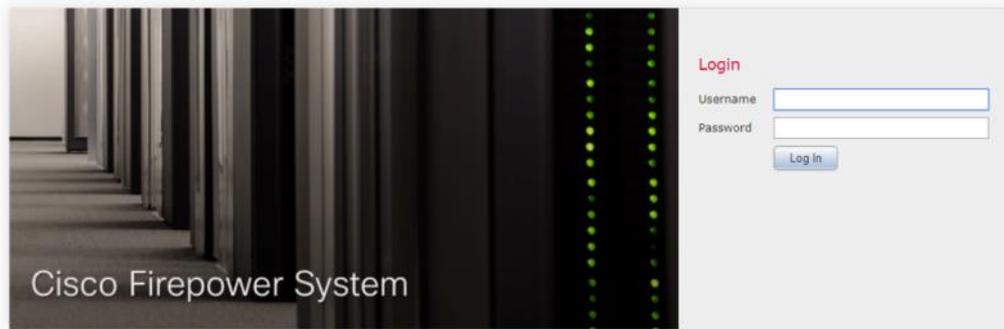
ステップ 2-2: 設定したIPアドレスにアクセス

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

※ ブラウザアクセスする端末の IP アドレスは、初期設定で変更した FMCのIPアドレスを同一セグメントのIPアドレスを使用 (ステップ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)



For technical/system questions, e-mail tac@ciscao.com
or call us at 1-800-553-2447 or 1-408-526-7209

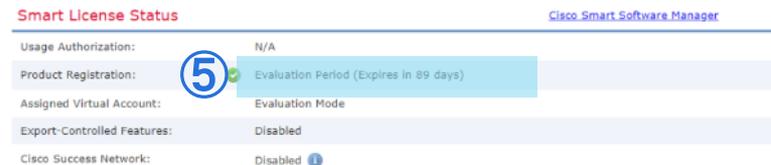
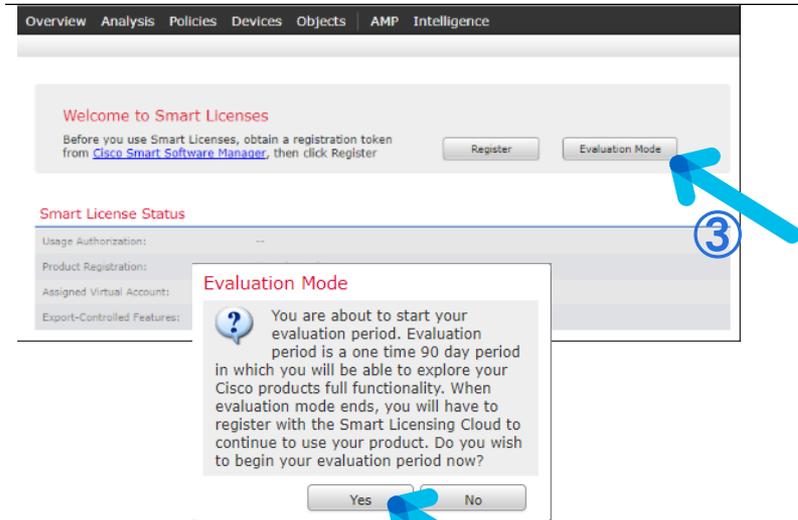
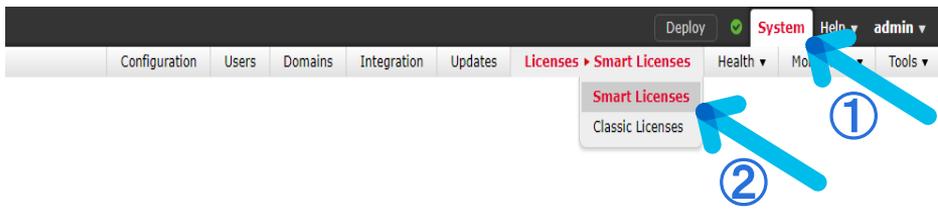




ステップ 3: ライセンスの追加

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

Select OVF and VMDK files

Select the OVF and VMDK files or OVA for the VM you would like to deploy

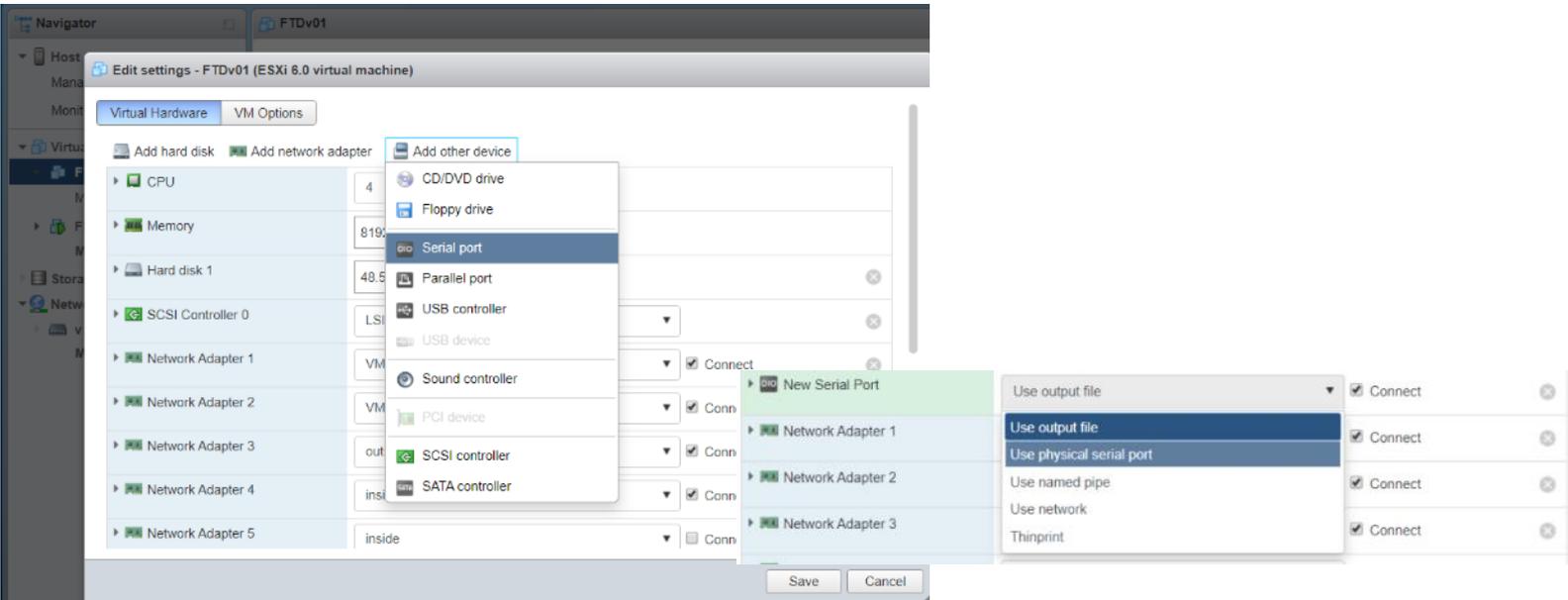
Enter a name for the virtual machine.

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

- ×  Cisco_Firepower_Threat_Defense_Virtual-ESXI-6.4.0-102.ovf
- ×  Cisco_Firepower_Threat_Defense_Virtual-6.4.0-102.vmdk

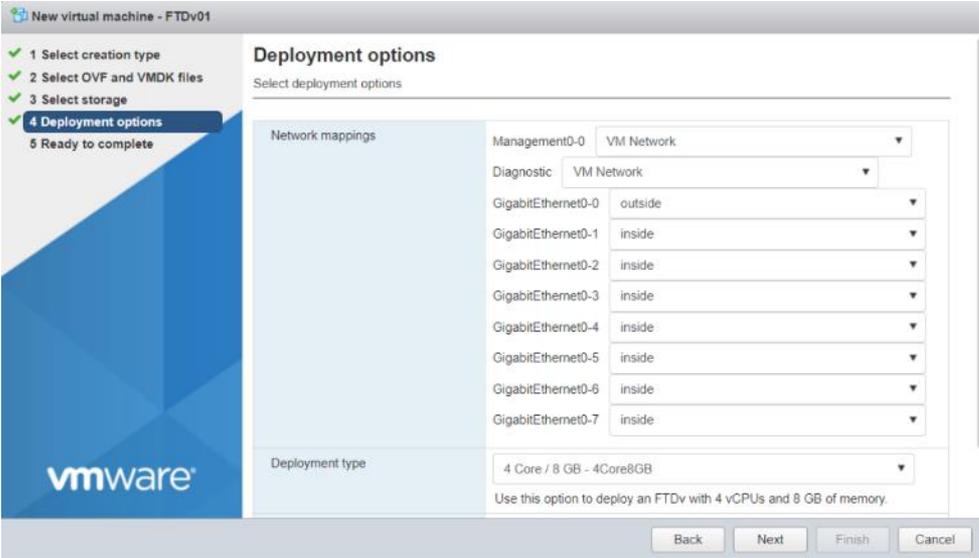
ステップ 1-3: OVFのデプロイ

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ーフェイスをここでは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 [SPACE] キーで最後まで表示させ、EULA合意を求める以下の表示に対して、“YES”を入力

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

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

- Adminユーザ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 [192.168.45.11]: 10.7
1.135.254
Enter a fully qualified hostname for this system [firepower]: FTD081
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220
.220]: 64.104.14.104
```

- 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.
```

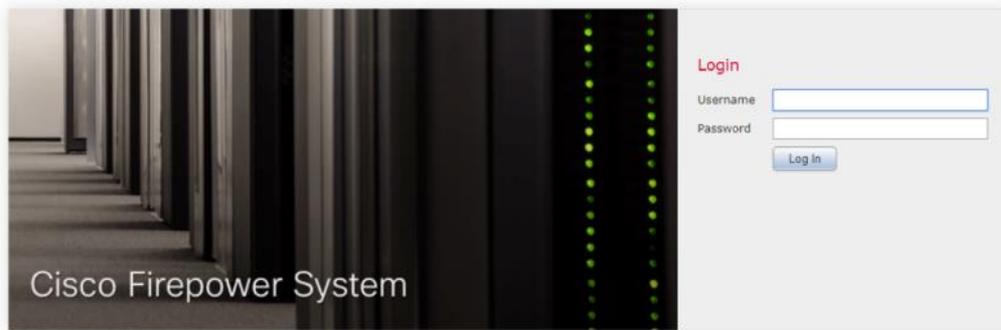


ステップ 1-1: FTDデバイスの登録

- ・ 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 ヘブラウザでHTTPSアクセスしログイン

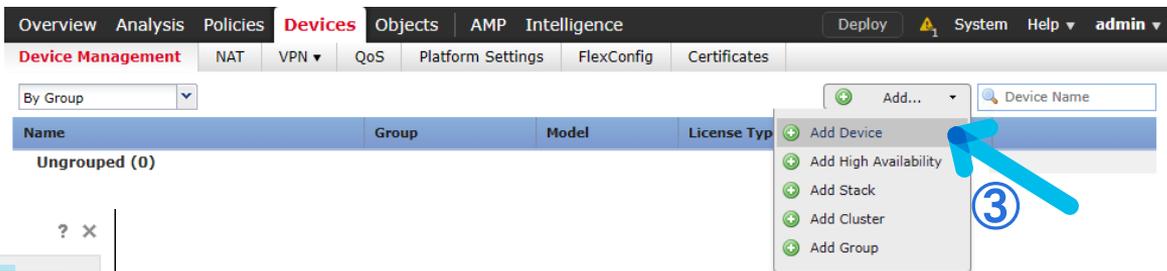
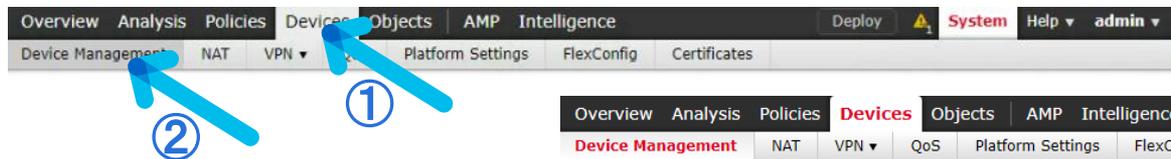


For technical/system questions, e-mail tac@cisico.com
or call us at 1-800-553-2447 or 1-408-526-7209





ステップ 1-2: FTDデバイスの登録



Add Device ? x

Host: 10.71.132.222

Display Name: FTDv01

Registration Key: cisco

Group: None

Access Control Policy: Create new policy

Smart Licensing: Create new policy

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



ステップ 1-3: FTDデバイスの登録

New Policy

Name: ACCESS-POLICY ①

Description:

Select Base Policy: None

Default Action: Block all traffic Intrusion Prevention Network Discovery

Save Cancel

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

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

Device Management

List of all the devices currently registered on the Firepower Management Center.

View By: Group All (1) Error (0) Warning (0) Offline (0) Normal (1) Deployment Pending (1) Add

Search Device

Name	Model	Ve...	Chassis	Licenses	Access Contro...
Ungrouped (1)					
FTDv01 10.71.132.222 - Routed	FTD for VMWare	6.4.0	N/A	Base, Threat (more...)	⑤

Add Device

Host: 10.71.132.222

Display Name: FTDv01

Registration Key: cisco

Group: None

Access Control Policy: ACCESS-POLICY

Smart Licensing

Malware ③

Threat

URL Filtering

Advanced

Unique NAT ID:

Transfer Packets

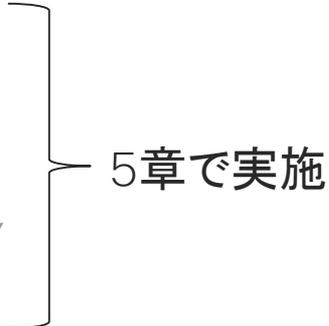
Register Cancel

- 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

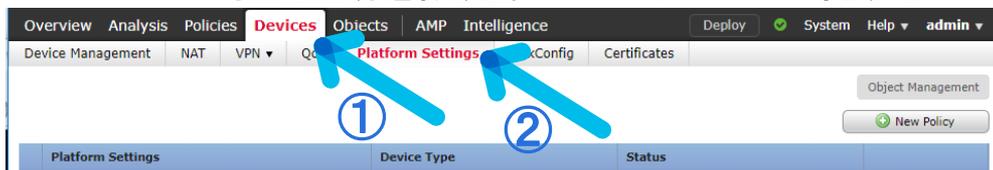
FTDとFMCその他初期設定に関して

- 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

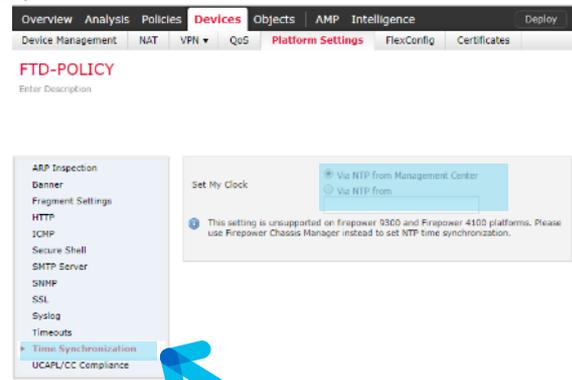
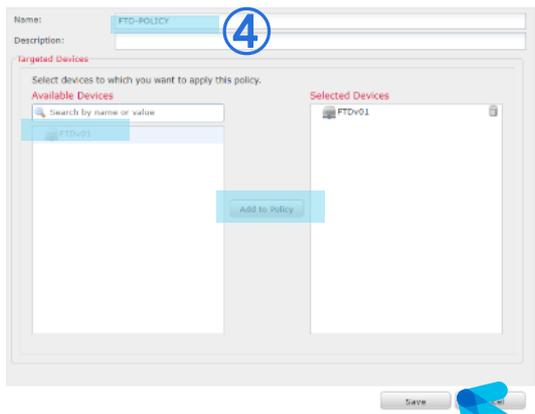


ステップ1-1 : Time Synchronization

- ・ FTDの時刻同期を設定。ここではFMCに従うものとする。



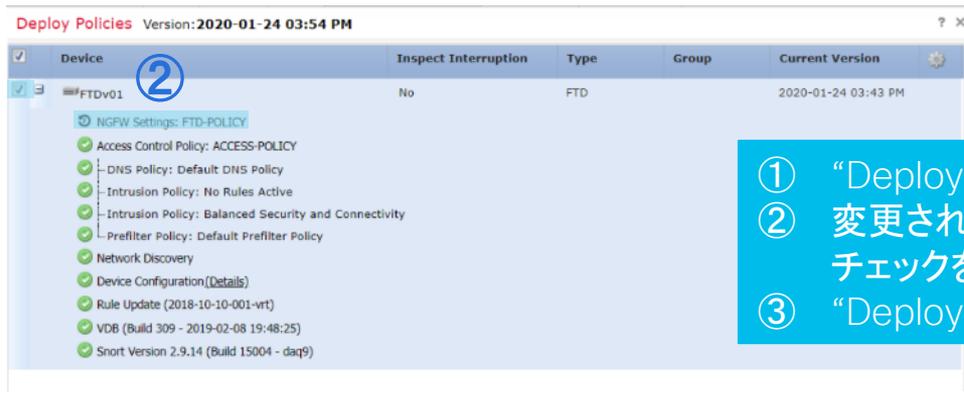
There are no policies created. Add a new [Firepower Settings Policy](#) (or) [Threat Defense Settings Policy](#)



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



ステップ1-2 : Time Synchronization



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

Selected devices: 1



(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

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

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

Device Management

List of all the devices currently registered on the Firepower Management Center

View By: Group All (1) Error (0) Warning (0) Offline (0) Normal (1) Deployment Pending (1) Add

Name	Model	Ve...	Chassis	Licenses	Access Contro...
FTDv01 10.71.122.222 - Routed	FTD for VMWare	6.4.0	N/A	Base, Threat (2 more...)	ACCESS-POLICY

Device Routing **Interfaces** Inline Sets DHCP

Search by name Sync Device Add Interfaces

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

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

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

FTDv

Cisco Firepower Threat Defense for VMWare

You have unsaved changes Save Cancel

Please save the configuration to make the changes available.

Device Routing **Interfaces** Inline Sets DHCP

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

Edit Physical Interface

General IPv4 IPv6 Advanced Hardware Configuration

Name: outside Enabled Management Only

Description:

Mode: None

Security Zone:

Interface ID: None

MTU: 1500

New Security Zone

Enter a name...
outside_zone

OK Cancel

General **IPv4** IPv6 Advanced Hardware Configuration

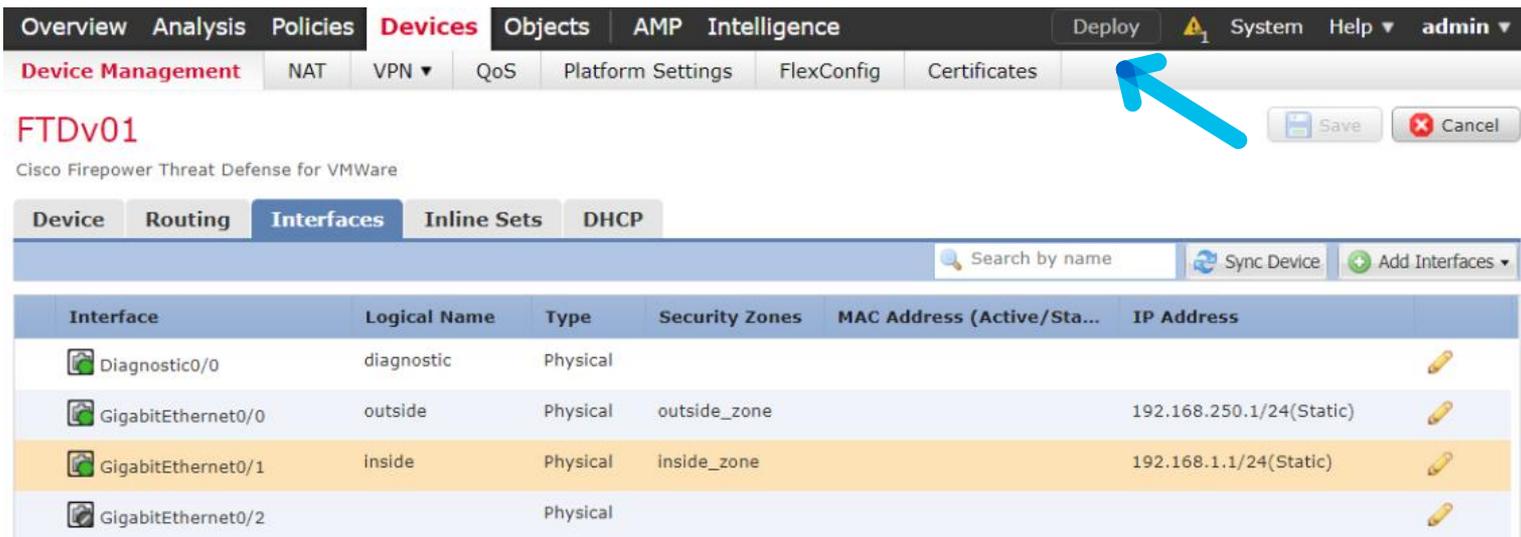
IP Type: Use Static IP

IP Address: 192.168.250.1/24

- 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 物理インターフェースの名前を入力し、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インターフェースとして設定し、saveする

ステップ2 : Interface設定

- Deployを押し設定を反映

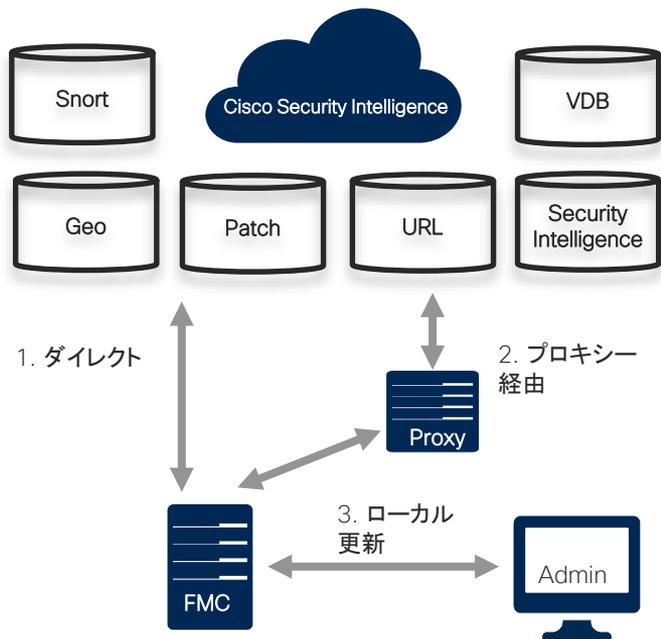


The screenshot shows the Cisco Firepower Threat Defense (FTD) configuration interface for device FTDv01. The top navigation bar includes tabs for Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. The 'Deploy' button is highlighted with a blue arrow. Below the navigation bar, the 'Device Management' section is visible, with sub-tabs for NAT, VPN, QoS, Platform Settings, FlexConfig, and Certificates. The main content area shows the 'Interfaces' tab selected, displaying a table of network interfaces. The table has columns for Interface, Logical Name, Type, Security Zones, MAC Address (Active/Sta...), and IP Address. The 'GigabitEthernet0/1' interface is highlighted in orange.

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Sta...	IP Address
Diagnostic0/0	diagnostic	Physical			
GigabitEthernet0/0	outside	Physical	outside_zone		192.168.250.1/24(Static)
GigabitEthernet0/1	inside	Physical	inside_zone		192.168.1.1/24(Static)
GigabitEthernet0/2		Physical			

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管理IPが閉域ネットワーク環境

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

更新パッケージおよび内容一覧

	内容	ファイル例	ワンタイム更新	定期更新	更新方法
Patch	新機能追加、既知Bug修正 (FMC/ FTD両方にパッチが存在)	Cisco_Firepower_Mgmt_C enter_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_Da tabase-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

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System ip admin

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools

Access List
Process
Audit Log Certificate
Audit Log
Login Banner
Change Reconciliation
DNS Cache
Dashboard
Database
External Database Access
Email Notification
Access Control Preferences
HTTPS Certificate
Information
Intrusion Policy Preferences
Console Configuration
Language

Management Interfaces

Network Analysis Policy Preferences
Remote Storage Device
REST API Preferences
SNMP
UCAPL/CC Compliance
Shell Timeout
Time
Time Synchronization
User Configuration
VMware Tools
Vulnerability Mapping
Web Analytics

Interfaces

Link	Name	Channels	MAC Address	IP Address
	eth0	Management Traffic Event Traffic	00:0C:29:2C:32:C1	10.71.132.221

Routes

IPv4 Routes

Destination	Netmask	Interface	Gateway
*			10.71.135.254

IPv6 Routes

Destination	Prefix Length	Interface	Gateway
-------------	---------------	-----------	---------

Shared Settings

Hostname: FMCv

Domains:

Primary DNS Server: 64.104.14.184

Secondary DNS Server:

Tertiary DNS Server:

Remote Management Port: 8305

ICMPv6

Allow Sending Echo Reply Packets:

Allow Sending Destination Unreachable Packets:

Proxy

Enabled:

HTTP Proxy: proxy.esl.cisco.com

Port: 80

Use Proxy Authentication:

Save Cancel

- 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

Software Download

Downloads Home / Security / Firewalls / Firewall Management / Firepower Management Center Virtual Appliance / Firepower Management Center Software- 6.4.0.7

Search...

Expand All Collapse All

Suggested Release

6.4.0.7

Latest Release

6.5.0.4

6.4.0.8

6.3.0.5

6.2.3.15

All Release

6.5

6.4

Firepower Management Center Virtual Appliance

Release 6.4.0.7

My Notifications

Related Links and Documentation

- Release Notes for 6.4.0.7
- Documentation Roadmap
- Hotfix Release Notes

File Information	Release Date	Size	
Cisco Firepower Mgmt Center Hotfix AA Do not untar	06-Jan-2020	1.71 MB	↓ 🛒
Cisco_Firepower_Mgmt_Center_Hotfix_AA-6.4.0.8-4.sh.REL.tar			
Cisco Firepower Mgmt Center Patch 6.4.0.7 Do not untar	19-Dec-2019	652.89 MB	↓ 🛒
Cisco_Firepower_Mgmt_Center_Patch-6.4.0.7-53.sh.REL.tar			

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

VDB/Patch ワンタイム更新

Overview Analysis Policies Devices Objects AMP Intelligence Deploy 2 System lp admin ▼

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

Product Updates Rule Updates Geolocation Updates

Upload Update

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	

Download updates

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

- 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
- 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	 

Product Updates Rule Updates Geolocation Updates

Currently running software version: 6.4.0

Selected Update

Type Cisco Firepower Mgmt Center Patch
Version 6.4.0.7-53
Date Tue Dec 17 22:30:03 UTC 2019
Release Notes
Reboot Yes

Download updates

①

- 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

▼ Ungrouped (1 total)

FMCv
10.71.132.221 - Cisco Firepower Management Center for VMWare v6.4.0

Health Policy
Initial_Health_Policy_2020-01-
20 21:57:03

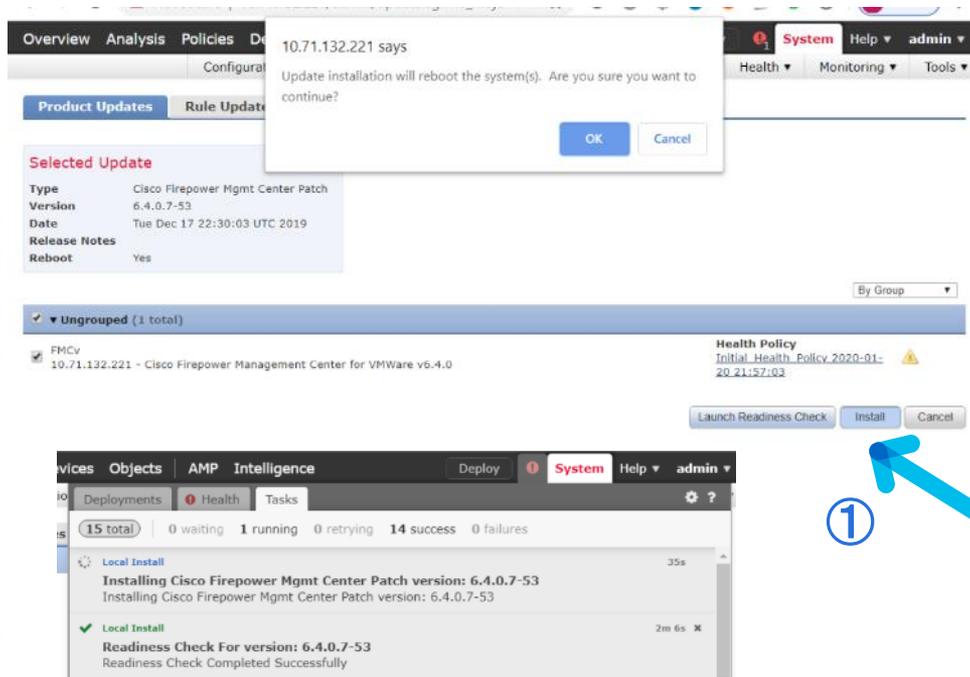
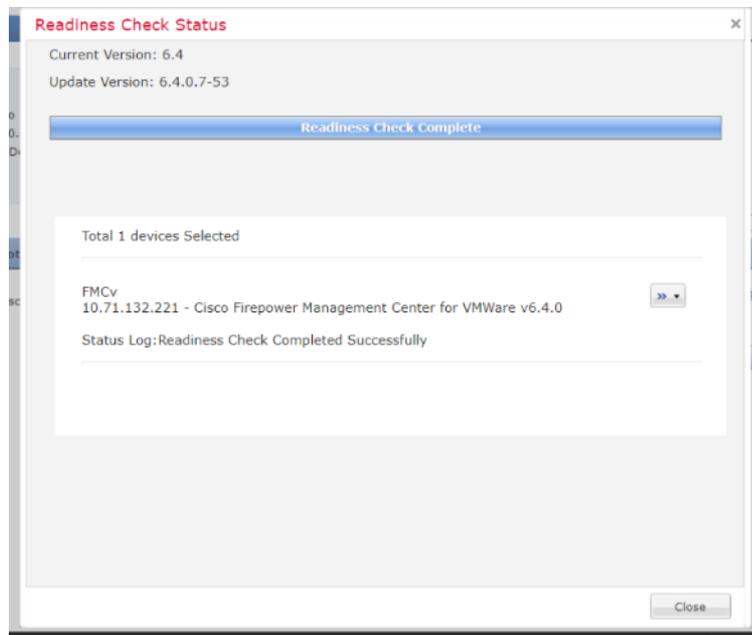
Launch Readiness Check Install Cancel

②

③

- 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 UMLare 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

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools

Currently running software version: 6.4.0.7

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 Firepower Mgmt Center Patch Uninstaller	6.4.0.7-53	Tue Dec 17 22:22:30 UTC 2019		Yes
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

Download updates

Hotfixの適用

Overview Analysis Policies Devices Objects AMP Intelligence Deploy **System** Help admin
Configuration Users Domains Integration **Updates** Licenses Health Monitoring Tools

Currently running software version: **6.4.0.7**

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 Firepower Mgmt Center Patch Uninstaller	6.4.0.7-53	Tue Dec 17 22:22:30 UTC 2019		Yes	 
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

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

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools > Scheduling

Add Task Today

New Task

Job Type: Download Latest Update ④

Schedule task to run: Once Recurring ⑤

Start On: March 27 2020 Asia/Tokyo

Repeat Every: 1 ⑥ Hours Days Weeks Months

Run At: 5:00 Pm

Repeat On: Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Job Name:

Update Items: ⑦ Software Vulnerability Database

Comment:

Email Status To: [Not available. You must set up your mail relay host.](#)

⑧ Save Cancel

- 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 定期更新 インストール

The screenshot shows the 'New Task' configuration page in the Cisco FMC console. The page is annotated with numbered callouts (1-9) and blue arrows pointing to specific UI elements. A blue callout box on the right contains a 9-step numbered list of instructions in Japanese.

- 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

GeoDB ワンタイム更新



One-Time Geolocation Update

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

Source

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

Download and install geolocation update from the Support Site
Import

Recurring Geolocation Updates

Enable Recurring Weekly Updates from the Support Site

Update Start Time

- 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



One-Time Geolocation Update

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

Source

Upload and install from file
ファイルを選択

Download and install from support site

Import

- 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

Recurring Geolocation Updates

Enable Recurring Weekly Updates from the Support Site ③

Update Start Time ④ Sunday 06:00 PM Asia/Tokyo

⑤ Save Cancel

Snort Rules ワンタイム更新

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools

Product Updates Rule Updates Geolocation Updates

Delete All Local Rules Rule Update Log

One-Time Rule Update/Rules Import

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

Source

Policy Deploy

Rule update or text rule file to upload and install (3)
ファイルを選択 選択されていません

Download new rule update from the Support Site (2)

Reapply all policies after the rule update import completes

Import

Warning

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

OK

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

- Reapply all policies After the rule update import completesにチェックすると、Snort Rules更新後、全ポリシーを持つFTDに対してルール配信 (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



Product Updates **Rule Updates** Geolocation Updates

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

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

Recurring Rule Update Imports

The scheduled rule update feature is not enabled.

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

Enable Recurring Rule Update Imports from the Support Site

Import Frequency

②
Daily at 11:00 PM Asia/Tokyo ③

Policy Deploy

Deploy updated policies to targeted devices after rule update completes

Save Cancel

Snort Rules 更新ログ

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools

Product Updates Rule Updates Geolocation Updates

Delete All Local Rules Rule Update Log

Summary	Time	User ID	Status	
Snort Rule Update 2020 03 30 001 vrt Completed install of Snort Rule Update 2020-03-30-001-vrt	2020-04-01 00:09:56	admin	✓	
Snort Rule Update 2020 03 25 001 vrt Completed install of Snort Rule Update 2020-03-25-001-vrt	2020-03-27 00:12:30	admin	✓	

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



Snort Rules 更新ログ

	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

Sid 1-35261

Rule Documentation

References

Rule Category

FILE-FLASH - Snort has detected suspicious traffic via the Adobe Flash Player. Flash is a common target of code execution, overflow, DoS, and memory corruption attacks in particular, via swf/s, action scripts, etc. Many networks block Flash altogether, the application will be deprecated in 2020.

Alert Message

FILE-FLASH | Adobe Flash Player remote code execution attempt



Snort Rules 更新ログ

Downloads Home / Security / Firewalls / Firewall Management / Firepower Management Center Virtual Appliance / Firepower SRU-VDB-GeoDB Content Updates- SRU

Firepower Management Center Virtual Appliance

Release SRU Related Links and Documentation
[Release Notes for SRU](#)

Secure Rule Updates are for 6.4 .

File Information	Release Date	Size
Cisco Secure Rule Update 2020-04-01-001 For Version 6.4 and later. Do not untar. Cisco_Firepower_SRU-2020-04-01-001-vrt.sh.REL.tar	02-Apr-2020	145.86 MB

Details

Description : Cisco Secure Rule Update 2020-04-01-001
For Version 6.4 and later. **Do not untar.**

Release : SRU

Release Date : 02-Apr-2020

FileName : Cisco_Firepower_SRU-2020-04-01-001-vrt.sh.REL.tar

Size : 145.86 MB (152944640 bytes)

MD5 Checksum : b11362004c31189bc16767f51c814138

SHA512 Checksum : 1127c9f72b9f5e4f4e40444158b...

[New Rules](#) [Modified Rules](#) [Secure SRU 2020-04-01-001](#) [Release Notes for SRU](#)

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:

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

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools

Cloud Services Realms Identity Sources eStreamer Host Input Client Smart Software Satellite Packet Analyzers

URL Filtering

Last URL Filtering Update: Apr 7, 2020 9:23 AM [Update Now](#)

Enable Automatic Updates

Query Cisco Cloud for Unknown URLs

Cached URLs Expire

Never

Save

AMP for Networks

Last Local Malware Detection Update: Apr 6, 2020 5:53 AM

Enable Automatic Local Malware Detection Updates

Share URI from Malware Events with Cisco

Use Legacy Port 32137 for AMP for Networks

Save

- 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

The screenshot shows the Cisco Security Intelligence Manager (SIM) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Objects' menu is expanded, showing 'Object Management' and 'Intrusion Rules'. Below the navigation, there are buttons for 'Update Feeds', 'Add Network Lists and Feeds', and a 'Filter' search box. The main content area is titled 'Network Lists and Feeds' and contains a table of network lists and feeds. The table has columns for 'Name', 'Type', and 'Last Updated'. The 'Security Intelligence' menu item in the left sidebar is highlighted with a red box.

Name	Type	Last Updated
Cisco-Intelligence-Feed <i>Last Updated: 2020-04-07 09:39:05</i>	Feed	
Cisco-TID-Feed <i>Last Updated: 2020-04-07 10:21:59</i>	Feed	
Global-Blacklist	List	
Global-Whitelist	List	

- 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

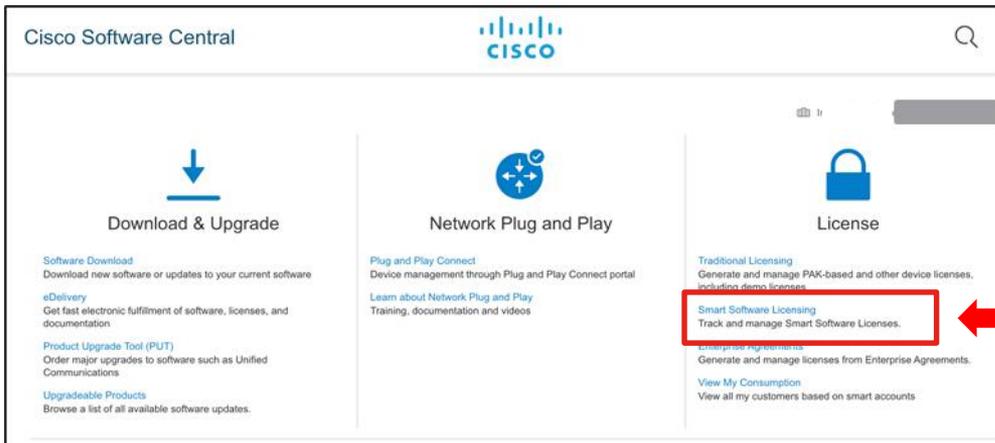
- デフォルト 2時間更新
-  マークを選択、定期更新時間を変更可能

4. スマートライセンスの適用

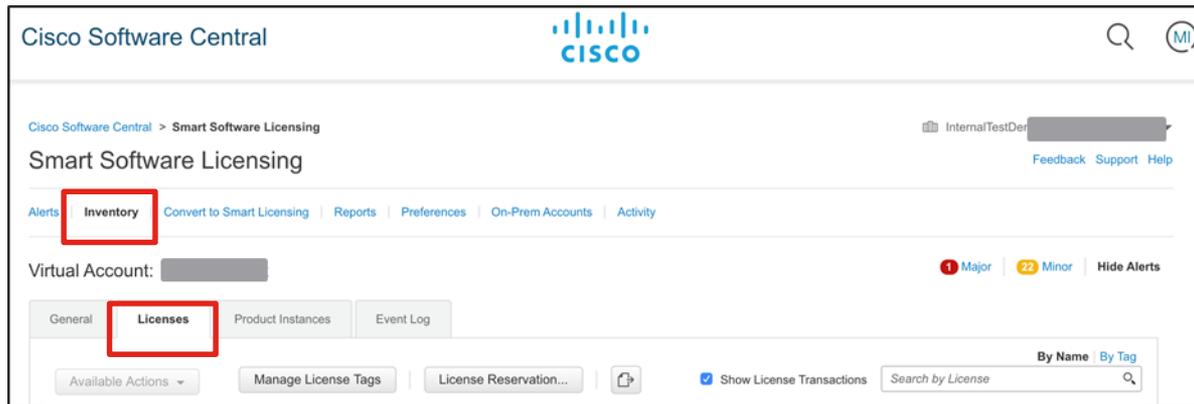
ステップ 1-1: CSSMにてライセンス確認

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

Cisco Software Central > Smart Software Licensing

Smart Software Licensing

Feedback Support Help

Alerts | Inventory | Convert to Smart Licensing | Reports | Preferences | On-Prem Accounts | Activity

Virtual Account: ← Virtual Account (VA) 1 Major | 22 Minor | Hide Alerts

General | **Licenses** | Product Instances | Event Log

Available Actions ▾ | Manage License Tags | License Reservation... | Show License Transactions | Search by License

Advanced Search ▾

<input type="checkbox"/>	License	Billing	Purchased	In Use	Balance	Alerts	Actions
<input checked="" type="checkbox"/>	C3650_24_Ipserv	Prepaid	1	0	+ 1		Actions ▾
<input checked="" type="checkbox"/>	C9500 DNA Advantage	Prepaid	3	0	+ 3	⚠ Licenses Expiring	Actions ▾
<input checked="" type="checkbox"/>	Firepower MCV Device License	Prepaid	20	2	+ 18	⚠ Licenses Expiring	Actions ▾
<input checked="" type="checkbox"/>	Firepower Threat Defense Base Features	Prepaid	2	2	0		Actions ▾
<input checked="" type="checkbox"/>	Threat Defense Virtual Malware Protection	Prepaid	4	0	+ 4	⚠ Licenses Expiring	Actions ▾
<input checked="" type="checkbox"/>	Threat Defense Virtual Threat Protection	Prepaid	6	0	+ 6	⚠ 2 Alerts	Actions ▾
<input checked="" type="checkbox"/>	Threat Defense Virtual URL Filtering	Prepaid	4	0	+ 4	⚠ Licenses Expiring	Actions ▾

Showing All 7 Records

Smart Account(SA) →

正常に付与されるとこちらに表示される。
”Purchasedの列に発行した個数分のライセンスが付与されているか確認。

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

Cisco Software Central > Smart Software Licensing

Smart Software Licensing

Alerts **Inventory** Convert to Smart Licensing | Reports | Preferences | On-Prem Ac

Virtual Account: [Redacted]

General Licenses Product Instances Event Log

Virtual Account

Description: test va account

Default Virtual Account: No

Product Instance Registration Tokens

The registration tokens below can be used to register new product instances to this virtual account.

New Token... ← **クリック**

Token	Expiration Date	Uses
-------	-----------------	------



Create Registration Token

This will create a token that is used to register product instances, so that they can use licenses from this virtual account. Once it's created, go to the Smart Licensing configuration for your products and enter the token, to register them with this virtual account.

Virtual Account: [Redacted]

Description: **FTD setup guide project** ← **任意で記入**

Expire After: **30** ← **有効期限日数を記入 (機器へトークンを入力し、その機器がCSSMIに初回アクセスするまでの有効日数)**

Between 1 - 365, 30 days recommended

Max. Number of Uses: [Empty field]

The token will be expired when either the expiration or the maximum uses is reached.

Allow export-controlled functionality on the products registered with this token

Create Token ← **クリック** Cancel

ステップ 1-4: Registration Token発行

Token	Expiration Date	Uses	Export-Controlled	Description	Created By	Actions
ODU5MmVhNzEtZDhk...	2020-Mar-21 03:17:22 (in 30...)		Allowed	FTD setup guide project		Actions
MWRjYTA5MGYtOTVi...	2020-Mar-06 01:17:48 (in 15...)		Allowed	FMC		Actions
OGEyNDliYWQtYzgxYi...	Expired		Allowed	cat9300_edge2		Actions
MDg4N2VjZWUtNzlyM...	Expired		Allowed			Actions

※最新のTokenが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

Welcome to Smart Licenses
Before you use Smart Licenses, obtain a registration token from [Cisco Smart Software Manager](#), then click Register

Smart License Status Cisco Smart Software Manager

Usage Authorization:	N/A
Product Registration:	✔ Evaluation Period (Expires in 63 days)
Assigned Virtual Account:	Evaluation Mode
Export-Controlled Features:	Disabled
Cisco Success Network:	Disabled ⓘ

Smart Licenses

License Type/Device Name	License Status	Device Type	Domain	Group
▶ Firepower Management Center Virtual (1)	✔			
▶ Base (1)	✔			
▶ Malware (1)	✔			
▶ Threat (1)	✔			
▶ URL Filtering (1)	✔			
AnyConnect Apex (0)				
AnyConnect Plus (0)				

Smart Licensing Product Registration

Product Instance Registration Token:
ODU5MmVhNzEtZDhkNi00NTRlTg1NTktNGl0MjZkYWJmNDg3LTE1ODQ3NjA2%0ANDIzODR8WndvZVkrVzd3U2V3MWIXcWtORCt4ekNpRjB4SVkvekt5VUd2QU1X%0AanhzUT0%3D%0A

ステップ1-4でCopyしたTokenをここに貼り付ける

If you do not have your ID token, you may copy it from your Smart Software Manager under the assigned virtual account. [Cisco Smart Software Manager](#)

Cisco Success Network

Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network. Check out the [sample data](#) that will be sent to Cisco.

Management Center establishes a secure connection to the Cisco Cloud so that it can participate in additional service offerings from Cisco such as technical support services and monitoring services. Management Center will establish and maintain this secure connection at all times. You can turn off this connection at any time by disabling Cisco Success Network. Disabling this will disconnect the device from the cloud.

Disconnection of Cisco Success Network will not impact the receipt of Updates or operation of the Smart Licensing capabilities; such functions will continue to operate normally.

Enable Cisco Success Network

任意。あとから変更も可能

Internet connection is required.

クリック → Apply Changes Cancel

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

Welcome to Smart Licenses

Before you use Smart Licenses, obtain a registration token from [Cisco Smart Software Manager](#), then click Register

Registering...

Deployments Health Tasks

20+ total | 0 waiting 1 running 0 retrying 20+ success 0 failures

Smart Licenses

Registration Registering U

Deploy System Help admin

Deployments Health Tasks

20+ total | 0 waiting 0 running 0 retrying 20+ success 0 failures

Smart Licenses

Registration to the Cisco Smart Software Manager

Registration was successful

Deploy System Help admin

3:34 until your session times out - localhost.cisco.com - VMware ESXi

Cisco Firepower Management Center for VMWare 6.4.0.7 Build 53 (FMCv) - admin

Overview Analysis Policies Devices Objects AMP Intelligence

Configuration Users Domains Integration Updates Licenses Smart Licenses Health Monitoring Tools

Smart License Status

[Cisco Smart Software Manager](#)

Usage Authorization: ✓ Authorized (Last Synchronized On Feb 20 2020)

Product Registration: ✓ Registered (Last Renewed On Feb 20 2020)

Assigned Virtual Account: ██████████

Export-Controlled Features: Enabled

Cisco Success Network: Enabled ⓘ

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

Smart License Status Cisco Smart Software Manager

Usage Authorization: ✖ Out of Compliance (Last Synchronized On Feb 20 2020) Re-Authorize

Product Registration: ✔ Registered (Last Renewed On Feb 20 2020)

Assigned Virtual Account:

Export-Controlled Features: Enabled

Cisco Success Network: Enabled ⓘ

コンプラ違反の表示。

登録自体は正常

Smart Licenses Filter

License Type/Device Name	License Status	Device Type	Domain	Group
▶ Firepower Management Center Virtual (2)	✔			
▶ Base (2)	✔			
▶ Malware (2)	ⓘ			
▶ Threat (2)	ⓘ			
▶ URL Filtering (2)	ⓘ			
AnyConnect Apex (0)				
AnyConnect Plus (0)				
AnyConnect VPN Only (0)				

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>

Note: Container Instances of same blade share feature licenses

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

} 2章で実施

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

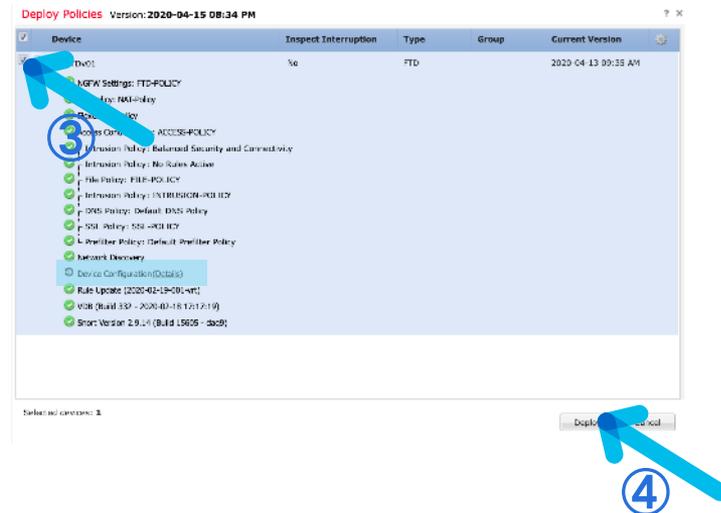
The image shows a sequence of screenshots from the Cisco FTD configuration interface, illustrating the steps to configure a static route. The steps are numbered 1 through 7:

- 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

The screenshots include:

- The main configuration window with the 'Routing' tab selected and the 'Add Route' button highlighted.
- The 'Add Static Route Configuration' dialog box where 'any-ipv4' is selected as the interface and the 'Add' button is highlighted.
- The 'Edit Network Object' dialog box where 'Host' is selected and '192.168.250.254' is entered as the network address.
- The 'Add Static Route Configuration' dialog box again, showing the 'Gateway' field with a plus sign highlighted.
- The 'Edit Network Object' dialog box with the 'Save' button highlighted.
- The 'Add Static Route Configuration' dialog box with the 'OK' button highlighted.

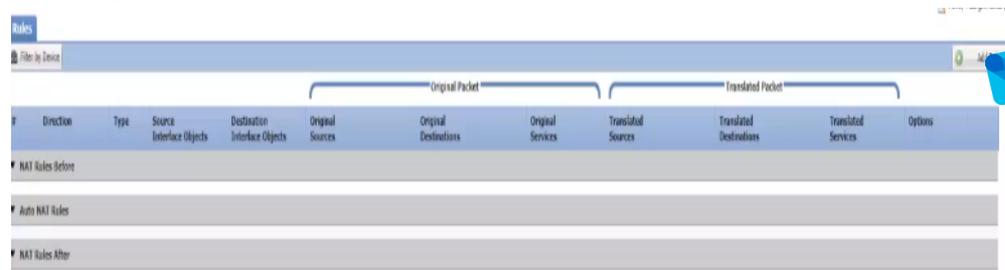
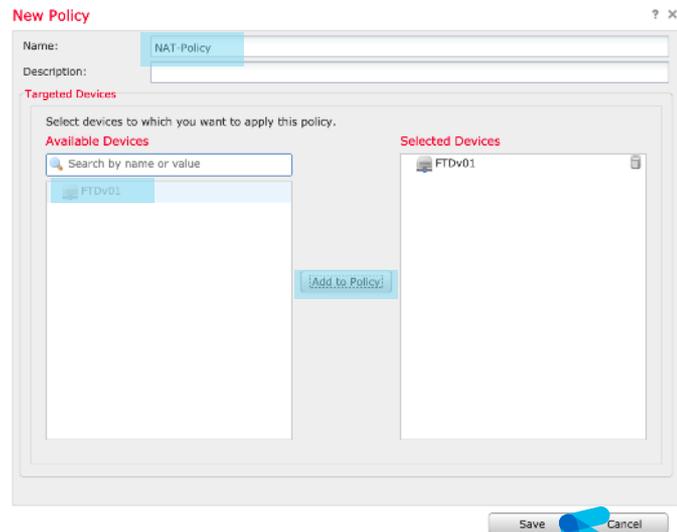
ステップ3-2 : Routing



- 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

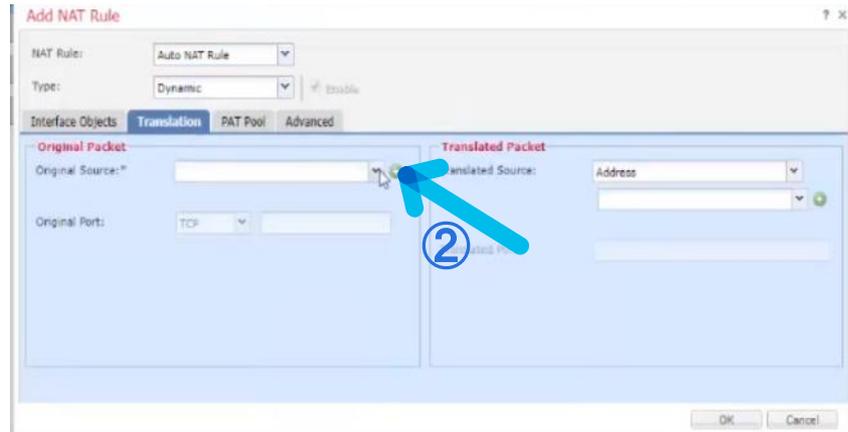
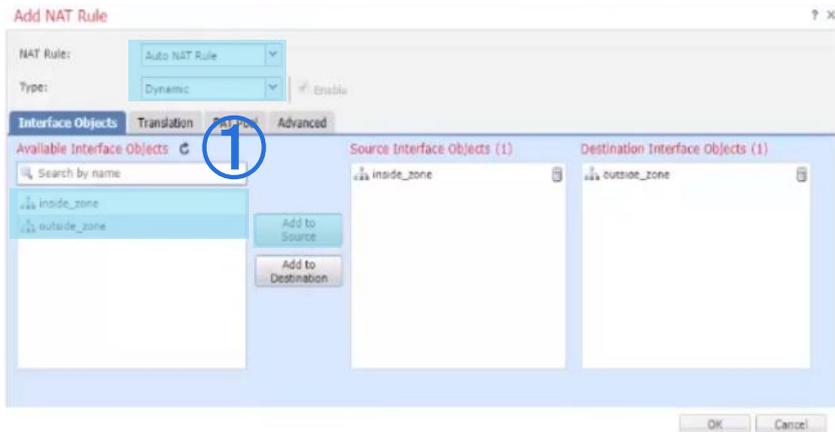
ステップ4-1 : NAT

- ・ FTDで行うNAT(PAT)を設定



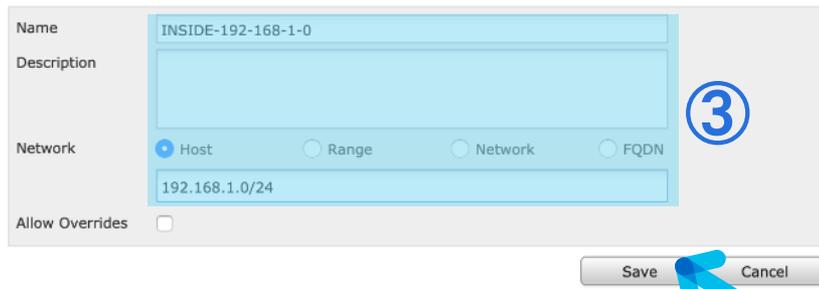
- ① Devicesを選択
- ② NATを選択
- ③ “Threat Defense NAT Policy”を選択
- ④ NAT Policyの名前、対象機器を選択し、“Save”
- ⑤ “Add”を選択

ステップ4-2 : NAT



New Network Object

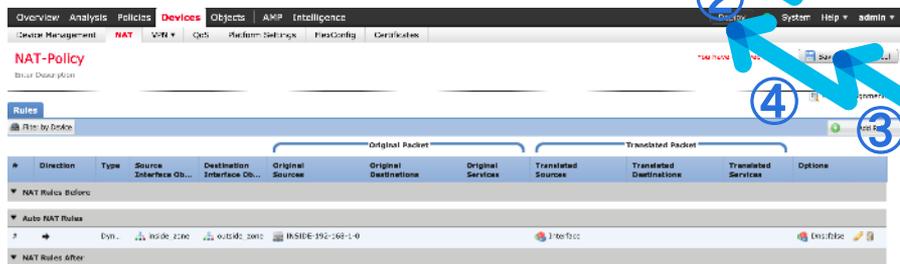
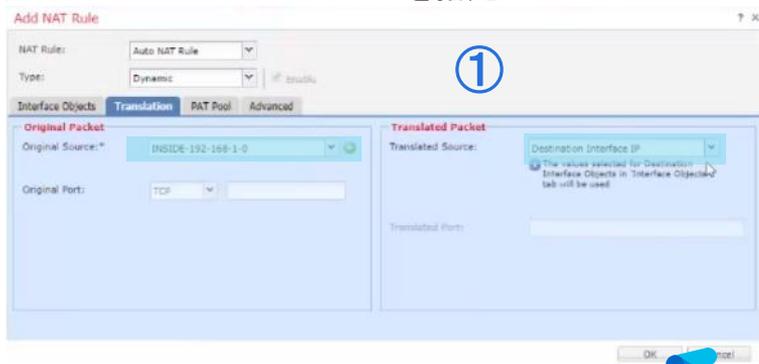
変換されるネットワークアドレス (ここでは 192.168.1.0/24) を登録



- 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

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

Access Control > Access Control Network Discovery Application Detectors Correlation Actions

Object Management Intrusion Network Analysis Policy DNS Import/Export

+ New Policy

Access Control Policy	Status	Last Modified
ACCESS-POLICY	Targeting 1 devices Up-to-date on all targeted devices	2020-04-08 17:02:26 Modified by "admin"

Rules Security Intelligence HTTP Responses Logging Advanced

Filter by Device Show Rule Conflicts Add Category Add Rule Search Rules

Name	Source Z...	Dest Zones	Source N...	Dest Net...	VLAN Tags	Users	Applicati...	Source P...	Dest Ports	URLs	ISE/SGT ...	Action
Mandatory - ACCESS-POLICY (-)												
There are no rules in this section. Add Rule or Add Category												
Default - ACCESS-POLICY (-)												
There are no rules in this section. Add Rule or Add Category												

Default Action Access Control: Trust All Traffic

Logging

Log at Beginning of Connection

Log at End of Connection

Send Connection Events to:

Event Viewer

Syslog Server (Using default syslog configuration in Access Control Logging) Show Overrides

SNMP Trap Select an SNMP Alert Configuration...

OK Cancel

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

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

Access Control Access Control Network Discovery Application Detectors Correlation Actions

ACCESS-POLICY You have unsaved changes Analyze Hit Counts Save Cancel

Enter Description

Deploy Policies Version: 2020-04-15 09:09 PM

Device	Inspect Interruption	Type	Group	Current Version
<input checked="" type="checkbox"/> FTDv01	No	FTD		2020-04-15 09:08 PM

NGFW Settings: FTD-POLICY
Intrusion Policy: NAT-Policy
FlexConnect Policy
Access Control Policy: ACCESS-POLICY
Intrusion Policy: Balanced Security and Connectivity
Intrusion Policy: No Rules Active
File Policy: FILE-POLICY
Intrusion Policy: INTRUSION-POLICY
DNS Policy: Default DNS Policy
SSL Policy: SSL-POLICY
Prefilter Policy: Default Prefilter Policy
Network Discovery
Device Configuration (Details)
Rule Update (2020-02-19-001-vrt)
VDB (Build 332 - 2020-02-18 17:17:19)
Snort Version 2.9.14 (Build 15605 - daq9)

Selected devices: 1

Deploy Cancel

- 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

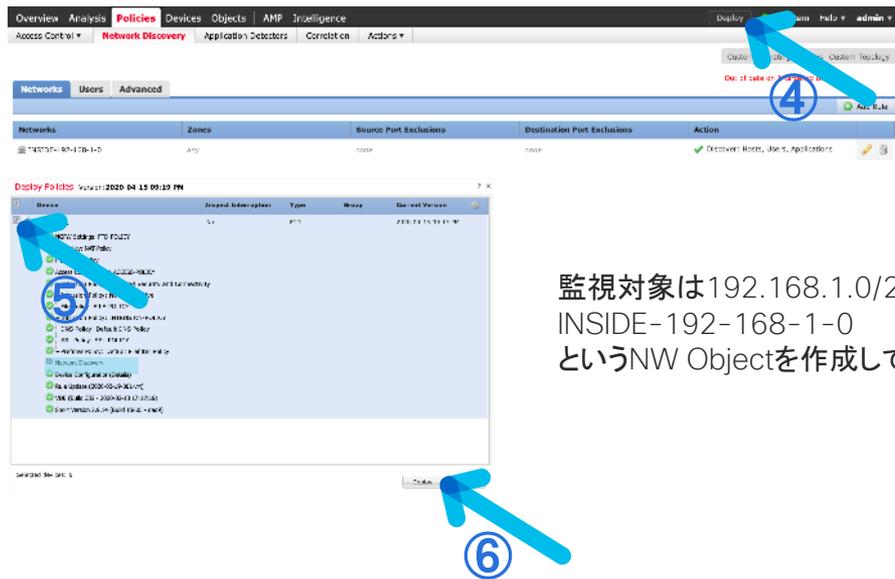
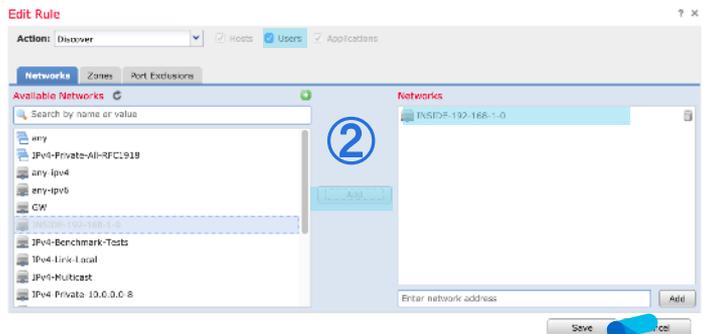
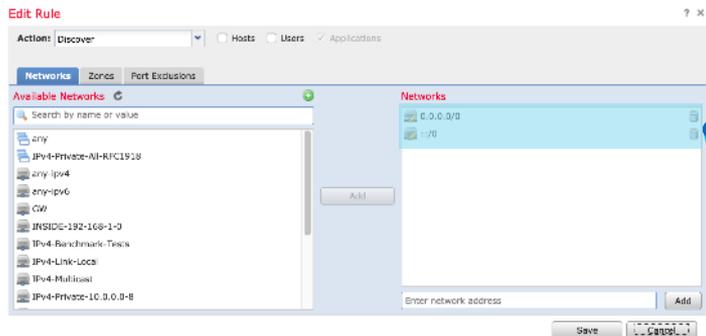
- Network Discovery Policyとは
 - 指定されたネットワーク内で、どのホスト、OS、アプリケーション等が存在するかを監視し、FMCで記憶していくためのポリシー
 - このポリシーでは監視する範囲を決め、その設定を有効にする

The screenshot shows the Cisco FMC interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Objects', 'AMP', and 'Intelligence'. The 'Policies' tab is active, and the 'Network Discovery' sub-tab is selected. A table lists the policy configuration for 'Discover: Applications'. A blue arrow labeled '1' points to the 'Policies' tab, a blue arrow labeled '2' points to the 'Network Discovery' sub-tab, and a blue arrow labeled '3' points to the pencil icon in the 'Action' column.

Networks	Zones	Source Port Exclusions	Destination Port Exclusions	Action
0.0.0.0/0 ::/0	any	none	none	Discover: Applications

- 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

Filter by IP and MAC addresses

Unique hosts: 1

Hosts [IPv4] (1)

- 192 (1)
 - 192.168 (1)
 - 192.168.1 (1)
 - 192.168.1.101**

Hosts [IPv6] (0)

Hosts [MAC] (0)

Host Profile

IP Addresses **192.168.1.101**

NetBIOS Name

Device (Hops) FTDv01 (0)

MAC Addresses (TTL) 00:0C:29:1A:88:DF (VMware, Inc.) (128)

Host Type Host

Last Seen 2020-04-15 21:11:32

Current User

View [Context Explorer](#) | [Connection Events](#) | [Intrusion Events](#) | [File Events](#) | [Malware Events](#)

Indications of Compromise (1) ▼

Category	Event Type	Description	First Seen	Last Seen
Malware Detected	Threat Detected in File Transfer	The host has encountered malware	2020-04-13 09:53:31	2020-04-13 10:40:10

Operating System ▼

Vendor	Product	Version	Source
Microsoft	Windows	7, Phone 7.5, 8	Firepower

Applications (73) ▼

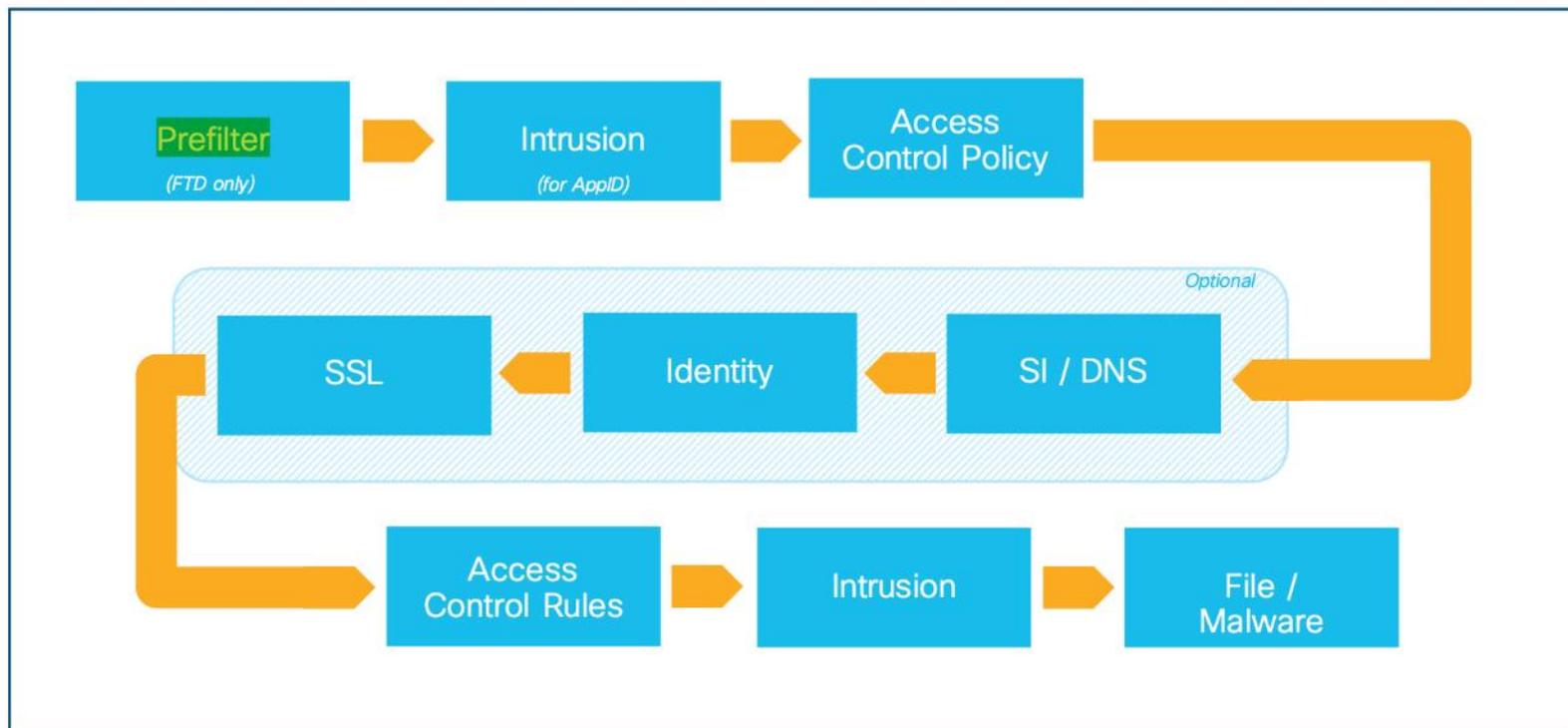
Application Protocol	Client	Version	Web Application
<input type="checkbox"/> SSL	<input type="checkbox"/> SSL client		<input type="checkbox"/> AOL Ads

- 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处理顺序概要



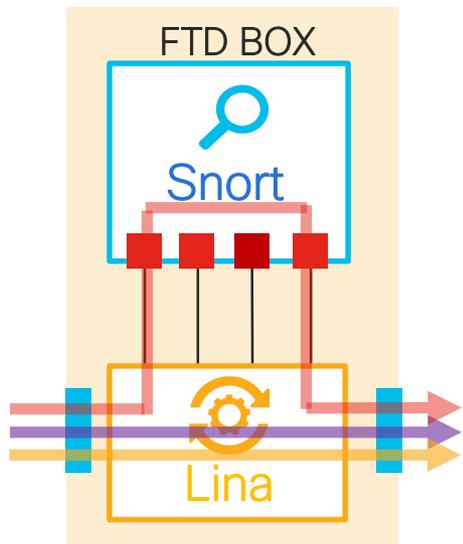
Prefilter概要

- 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)

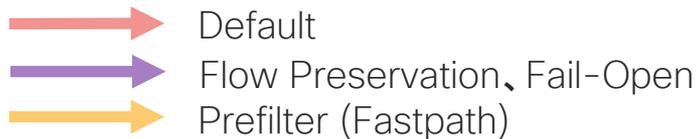
【Prefilterの利用ケース例】

- 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



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)	全ての接続で対応
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 src=192.168.75.39 dst=192.168.76.39	GRE Header	Inner IP Header src=10.0.0.1 dst=10.0.0.2	L7
-----------	-----------------------------------------------------------	------------	-------------------------------------------------	----

Access Control Policyは内部IPヘッダを参照

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

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

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

Access Control ▶ **Prefilter** Network Discovery Application Detectors Correlation Actions ▼

Object Management Access Control + New Policy

Prefilter Policy	Domain	Last Modified
Default Prefilter Policy Default Prefilter Policy with default action to allow all tunnels	Global	2019-04-11 15:53:01 Modified by "admin"

New Policy

Name:

Description:

Save Cancel

- ① Policiesを選択
- ② Prefilterを選択
- ③ New Policyを選択
- ④ 任意の名前とDescription(Optional)を入力
- ⑤ "Save"を選択

ステップ2-2 : Prefilter(Prefilter Rule)の作成

Access Control ▸ Prefilter Network Discovery Application Detectors Correlation Actions ▾

Object Management Access Control

+ New Policy

Filter Policy	Domain	Last Modified	
Default Prefilter Policy Default Prefilter Policy with default action to allow all tunnels	Global	2020-04-07 09:25:35 Modified by "admin"	 
Test Prefilter Test	Global	2020-04-06 22:43:08 Modified by "admin"	 

Access Control ▸ Prefilter Network Discovery Application Detectors Correlation Actions ▾

Test Prefilter

Test

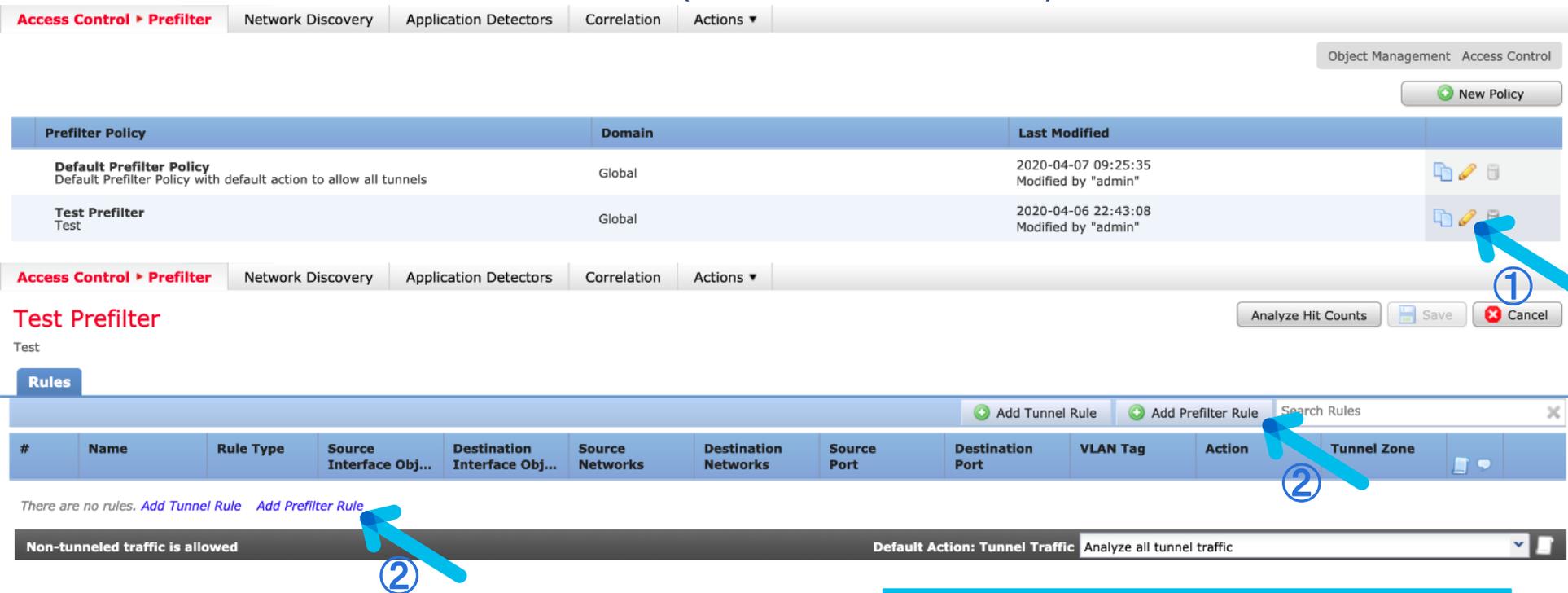
Analyze Hit Counts Save Cancel

Rules

+ Add Tunnel Rule + Add Prefilter Rule Search Rules

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

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



- ① 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

Add Prefilter Rule

① Prefilter rules perform early handling of traffic based on simple network characteristics. Fastpathed traffic bypasses access control and QoS.

Name: Test Prefilter Rule Src

Action: Fastpath

Insert: below rule

Interface Objects: Networks

Available Networks:

- any
- IPv4-Private-All-RFC1918
- any-ipv4
- any-ipv6
- GW
- INSIDE-192-168-1-0
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8

Source Networks (0): any

Destination Networks (0): any

Buttons: Add to Source, Add to Destination, Add, Cancel

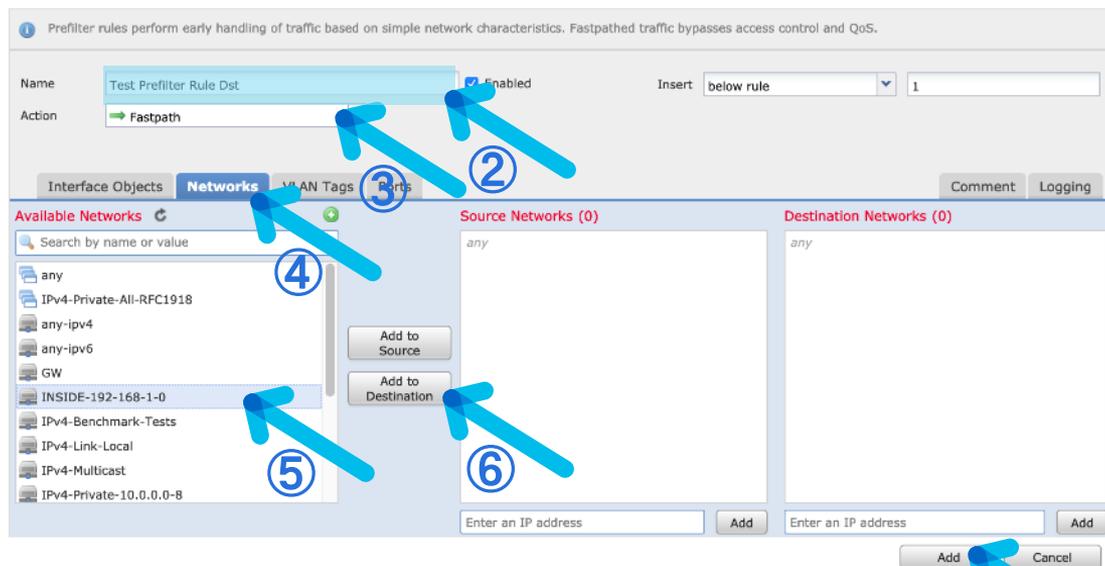
1行目のruleを作成

- 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



Add Prefilter Rule



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

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

Access Control > Prefilter Network Discovery Application Detectors Correlation Actions

You have unsaved changes Analyze Hit Counts Save Cancel

Test:

Rules

#	Name	Rule Type	Source Interface Obj...	Destination Interface Obj...	Source Networks	Destination Networks	Source Port	Destination Port	VLAN Tag	Action	Tunnel Zone
1	Test Prefilter Rule S Prefilter	any	any	any	INSIDE-192.168	any	any	any	any	Fastpath	na
2	Test Prefilter Rule L Prefilter	any	any	any	INSIDE-192.168	any	any	any	any	Fastpath	na

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

Access Control Policyにこの Prefilter Policyを紐つける

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

Access Control > Access Control Network Discovery Application Detectors Correlation Actions

Object Management Intrusion Network Analysis Policy DNS Export/Import

+ New Policy

Access Control Policy	Status	Last Modified
ACCESS-POLICY	Targeting 1 devices Up-to-date on all targeted devices	2020-04-03 19:24:38 Modified by 'admin'

Prefilter Policy ? X

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

Test Prefilter

OK Cancel

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

Access Control > Access Control Network Discovery Application Detectors Correlation Actions

Analyze Hit Counts Save Cancel

Enter Description

Prefilter Policy: Default Prefilter Policy SSL Policy: SSL-POLICY Identity Policy: IDENTITY

- 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

The screenshot shows the Cisco ASA configuration interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Policies' tab is active, showing 'ACCESS-POLICY'. A 'Save' button is highlighted with a blue arrow and a circled '1'. Below this, the 'Deploy' button is highlighted with a blue arrow and a circled '2'. A dialog box titled 'Deploy Policies' is open, showing a table of devices and their configurations. The 'Device' column has a checked box for 'FTDv01'. A blue arrow and a circled '3' point to this checkbox. The 'Current Version' column shows '2020-04-07 09:25 AM'. The 'Deploy Policies' dialog lists various policies, including 'NGFW Settings: FTD-POLICY', 'NAT Policy: NAT-POLICY', 'Access Control Policy: ACCESS-POLICY', 'Intrusion Policy: Balanced Security and Connectivity', 'Intrusion Policy: No Rules Active', 'File Policy: FILE-POLICY', 'Intrusion Policy: INTRUSION-POLICY', 'DNS Policy: Default DNS Policy', 'SSL Policy: SSL-POLICY', and 'Prefilter Policy: Test.Prefilter'. At the bottom of the dialog, the 'Deploy' button is highlighted with a blue arrow and a circled '4'. The 'Selected devices: 1' text is visible at the bottom left of the dialog.

Device	Inspect Interruption	Type	Group	Current Version
<input checked="" type="checkbox"/> FTDv01	No	FTD		2020-04-07 09:25 AM

- NGFW Settings: FTD-POLICY
- NAT Policy: NAT-POLICY
- Access Control Policy: ACCESS-POLICY
- Intrusion Policy: Balanced Security and Connectivity
- Intrusion Policy: No Rules Active
- File Policy: FILE-POLICY
- Intrusion Policy: INTRUSION-POLICY
- DNS Policy: Default DNS Policy
- SSL Policy: SSL-POLICY
- Prefilter Policy: Test.Prefilter
- Network Discovery
- Device Configuration (Details)
- Rule Update (2020-02-19-001-vrt)
- VDB (Build 332 - 2020-02-18 17:17:19)
- Smart Version 2.9.14 (Build 15605 - daq9)

Selected devices: 1

Deploy CANCEL

- 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)

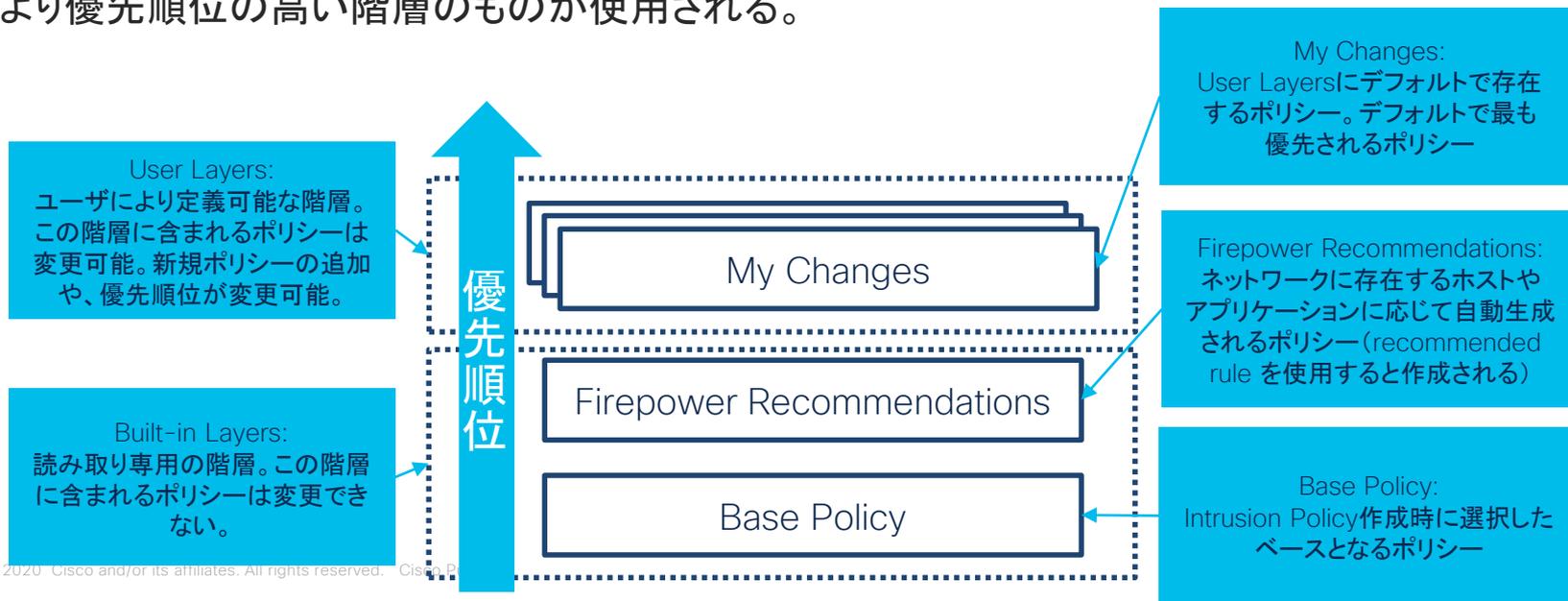
Intrusion Policyにはシグネチャに対するパラメータが含まれ、トラフィックに対するIPSの振る舞いを制御する。

■シグネチャのパラメータ

項目	パラメータ	説明
Rule State	<ul style="list-style-type: none">• Generate Events• Drop and Generate Events• Disable• Inherit	シグネチャヒット時の動作設定
Event Filtering	<ul style="list-style-type: none">• 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。Built-in Layersは読み取り専用なためユーザがポリシーの内容や順番を変更できるのはUser Layersに含まれるポリシーのみである。ポリシー間で異なるパラメータが競合する場合はより優先順位の高い階層のものが使用される。



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



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

- Name ***: A text input field containing 'INTRUSION-POLICY'. A blue arrow labeled '4' points to this field.
- Description**: An empty text input field.
- Drop when Inline**: A checkbox that is unchecked. A blue arrow labeled '5' points to this checkbox.
- Base Policy**: A dropdown menu showing 'Balanced Security and Connectivity'. A blue arrow labeled '6' points to the 'Create and Edit Policy' button at the bottom right of the dialog.

At the bottom of the dialog, there are three buttons: 'Create Policy', 'Create and Edit Policy', and 'Cancel'. A blue arrow labeled '6' points to the 'Create and Edit Policy' button.

- 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

Edit Policy: INTRUSION-POLICY

Policy Information < Back

Policy Information

Name: INTRUSION-POLICY

Description:

Drop when Inline:

Base Policy | Balanced Security and Connectivity Manage Base Policy

The base policy is up to date (Rule Update 2020-02-19-001-vrt)

This policy has 15356 enabled rules Manage Rules

30 rules generate events View

15326 rules drop and generate events View

[No recommendations have been generated. Click here to set up Firepower recommendations.](#)

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

Edit Policy: INTRUSION-POLICY

Rules

Rule Configuration

Rule Content

Category

app-detect

browser-chrome

browser-firefox

browser-ie

browser-other

browser-plugins

browser-webkit

content-replace

decoder

exploit-kit

file-executable

file-flash

file-identify

file-image

file-java

Classifications

Microsoft Vulnerabilities

Microsoft Worms

Platform Specific

Preprocessors

Priority

Rule Update

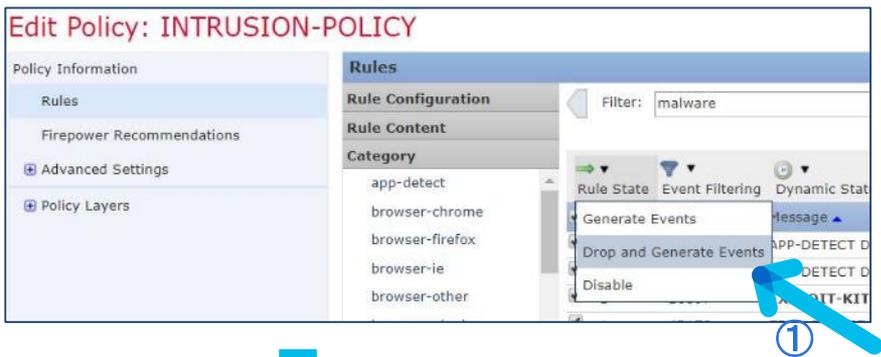
Filter: malware

6286 selected rules of 6286

Rule State	Event Filtering	Dynamic State	Alerting	Comments
<input checked="" type="checkbox"/>	SID		Message	
<input checked="" type="checkbox"/>	28069		APP-DETECT DNS request for potential malware SafeGuard to domain 360.cn	
<input checked="" type="checkbox"/>	2070		APP-DETECT DNS request for potential malware SafeGuard to domain 360safe.com	
<input checked="" type="checkbox"/>	2689		EXPLOIT-KIT Flashpack/Safe/CritX exploit kit malware download	
<input checked="" type="checkbox"/>	43179		FILE-OFFICE Powerpoint mouseover powershell malware download attempt	
<input checked="" type="checkbox"/>	43180		FILE-OFFICE Powerpoint mouseover powershell malware download attempt	
<input checked="" type="checkbox"/>	21489		FILE-OTHER Microsoft Windows chm file malware related exploit	
<input checked="" type="checkbox"/>	39851		INDICATOR-COMPROMISE Connection to malware sinkhole - CERT.PL	
<input checked="" type="checkbox"/>	31214		INDICATOR-COMPROMISE connection to zeus malware sinkhole	
<input checked="" type="checkbox"/>	33215		INDICATOR-COMPROMISE DNS request for known malware domain icanhazip.com	
<input checked="" type="checkbox"/>	33216		INDICATOR-COMPROMISE DNS request for known malware domain tor2web.org	
<input checked="" type="checkbox"/>	44037		INDICATOR-COMPROMISE DNS request for known malware sinkhole domain iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com - WannaCry	
<input checked="" type="checkbox"/>	17812		INDICATOR-COMPROMISE potential malware - download of fexplore.exe	
<input checked="" type="checkbox"/>	17813		INDICATOR-COMPROMISE potential malware - download of iprinp.dll	
<input checked="" type="checkbox"/>	17810		INDICATOR-COMPROMISE potential malware - download of server32.exe	
<input checked="" type="checkbox"/>	17811		INDICATOR-COMPROMISE potential malware - download of svchost.exe	
<input checked="" type="checkbox"/>	17814		INDICATOR-COMPROMISE potential malware - download of winzf32.dll	
<input checked="" type="checkbox"/>	30997		INDICATOR-COMPROMISE Potential malware download - .doc.exe within .zip file	
<input checked="" type="checkbox"/>	30998		INDICATOR-COMPROMISE Potential malware download - .gif.exe within .zip file	
<input checked="" type="checkbox"/>	30999		INDICATOR-COMPROMISE Potential malware download - .jpg.exe within .zip file	

- 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动設定④

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

Access Control > Intrusion Network Discovery Application Detectors Correlation Actions

Edit Policy: INTRUSION-POLICY

Policy Information

- Rules
- Firepower Recommendations
- Advanced Settings
- Policy Layers

Rules

Rule Configuration Filter: Category:"exploit-kit" 747 selected rules of 747

Rule Content

Category

- app-detect
- browser-chrome
- browser-firefox
- browser-ie
- browser-other
- browser-plugins
- browser-webkit
- content-replace
- decoder
- exploit-kit**
- file-executable
- file-flash
- file-identify
- file-image
- file-java

Classifications

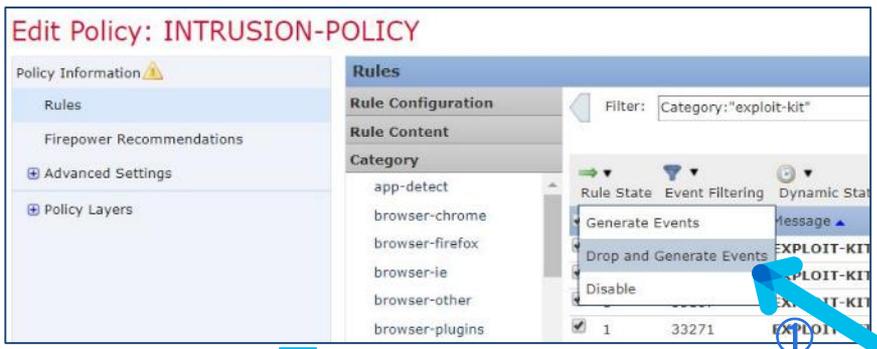
- Microsoft Vulnerabilities
- Microsoft Worms
- Platform Specific
- Preprocessors
- Priority
- Rule Update

Rule State	Event Filtering	Dynamic State	Alerting	Comments
<input checked="" type="checkbox"/>	SID			Message
<input checked="" type="checkbox"/>	33184			EXPLOIT-KIT Angler exploit kit Adobe Flash download
<input checked="" type="checkbox"/>	33187			EXPLOIT-KIT Angler exploit kit Adobe Flash encoded shellcode detected
<input checked="" type="checkbox"/>	33187			EXPLOIT-KIT Angler exploit kit Adobe Flash SWF exploit download
<input checked="" type="checkbox"/>	33271			EXPLOIT-KIT Angler exploit kit Adobe Flash SWF exploit download
<input checked="" type="checkbox"/>	33272			EXPLOIT-KIT Angler exploit kit Adobe Flash SWF exploit download
<input checked="" type="checkbox"/>	33186			EXPLOIT-KIT Angler exploit kit Adobe Flash SWF exploit download
<input checked="" type="checkbox"/>	33274			EXPLOIT-KIT Angler exploit kit Adobe Flash SWF exploit download
<input checked="" type="checkbox"/>	33286			EXPLOIT-KIT Angler exploit kit Adobe Flash SWF exploit download
<input checked="" type="checkbox"/>	33273			EXPLOIT-KIT Angler exploit kit Adobe Flash SWF exploit download
<input checked="" type="checkbox"/>	36071			EXPLOIT-KIT Angler exploit kit browser version detection attempt
<input checked="" type="checkbox"/>	36802			EXPLOIT-KIT Angler exploit kit browser version detection attempt
<input checked="" type="checkbox"/>	38682			EXPLOIT-KIT Angler Exploit Kit email gate
<input checked="" type="checkbox"/>	31331			EXPLOIT-KIT Angler exploit kit encrypted binary download
<input checked="" type="checkbox"/>	31130			EXPLOIT-KIT Angler exploit kit encrypted binary download
<input checked="" type="checkbox"/>	31694			EXPLOIT-KIT Angler exploit kit encrypted binary download
<input checked="" type="checkbox"/>	29414			EXPLOIT-KIT Angler exploit kit encrypted binary download
<input checked="" type="checkbox"/>	29413			EXPLOIT-KIT Angler exploit kit encrypted binary download
<input checked="" type="checkbox"/>	31695			EXPLOIT-KIT Angler exploit kit encrypted binary download
<input checked="" type="checkbox"/>	33185			EXPLOIT-KIT Angler

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动設定⑥

Edit Policy: INTRUSION-POLICY

Policy Information ⚠

- Rules
- Firepower Recommendations
- Advanced Settings
- Policy Layers

Rules

Rule Configuration

Rule Content

Category

app-detect

browser-chrome

browser-firefox

browser-ie

browser-other

browser-plugins

browser-webkit

content-replace

decoder

exploit-kit

file-executable

file-flash

file-identify

file-image

file-java

Classifications

Microsoft Vulnerabilities

Microsoft Worms

Platform Specific

Preprocessors

Priority

Rule Update

Filter: ICMP

1 selected rule of 203

Rule State	Event Filtering	Dynamic State	Alerting	Comments
GID	SID	Message		
1	374	PROTOCOL-ICMP PING IP NetMonitor Macintosh		
1	375	PROTOCOL-ICMP PING LINUX/"BSD		
1	376	PROTOCOL-ICMP PING Microsoft Windows		
1	377	PROTOCOL-ICMP PING Network Toolbox 3 Windows		
1	381	PROTOCOL-ICMP PING Oracle Solaris		
1	378	PROTOCOL-ICMP PING Ping-O-MeterWindows		
1	379	PROTOCOL-ICMP PING Pinger Windows		
1	380	PROTOCOL-ICMP PING Seer Windows		
1	484	PROTOCOL-ICMP PING Sniffer Pro/NetXRay network scan		
1	480	PROTOCOL-ICMP PING speedera		
1	365	PROTOCOL-ICMP PING undefined code		
1	366	PROTOCOL-ICMP PING Unix		
1	482	PROTOCOL-ICMP PING WhatsupGold Windows		
1	382	PROTOCOL-ICMP PING Windows		
1	384	PROTOCOL-ICMP PING Windows		
1	8730	PROTOCOL-ICMP record denial of service attempt		
1	436	PROTOCOL-ICMP Redirect for OS and Network		
1	437	PROTOCOL-ICMP Redirect for OS and Network		
1	438	PROTOCOL-ICMP Redirect undefined code		

- 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

Edit Policy: INTRUSION-POLICY

Policy Information

- Rules
- Firepower Recommendations
- Advanced Settings
- Policy Layers

Rules

Rule Configuration

Rule Content

Category

app-detect

browser-chrome

browser-firefox

browser-ie

browser-other

browser-plugins

browser-webkit

content-replace

decoder

exploit-kit

file-executable

file-flash

file-identify

file-image

Filter: eicar

6 selected rules of 6

Rule State	Event Filtering	Dynamic State	Alerting	Comments	Policy
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GID	SID	Message			
<input checked="" type="checkbox"/> 1	42374	POLICY-OTHER eicar file detected			
<input checked="" type="checkbox"/> 1	42375	POLICY-OTHER eicar file detected			
<input checked="" type="checkbox"/> 1	42375	POLICY-OTHER eicar file detected			
<input checked="" type="checkbox"/> 1	42376	POLICY-OTHER eicar file detected			
<input checked="" type="checkbox"/> 1	42373	POLICY-OTHER eicar file detected			
<input checked="" type="checkbox"/> 1	37732	POLICY-OTHER eicar test string download attempt			

- 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



Success

Successfully set the rule state for 6 rule(s)

OK

- 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

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

Access Control ▶ Intrusion Network Discovery Application Detectors Correlation Actions ▼

Edit Policy: INTRUSION-POLICY

Policy Information < Back

Rules

Firepower Recommendations 1

Advanced Settings

Policy Layers

Name: INTRUSION-POLICY

Description:

Drop when Inline:

Base Policy: Balanced Security and Connectivity Manage Base Policy

The base policy is up to date (Rule Update 2018-10-10-001-vrt)

This policy has 13744 enabled rules Manage Rules

31 rules generate events View

13713 rules drop and generate events View

[No recommendations have been generated. Click here to set up Firepower recommendations.](#)

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

Commit Changes Discard Changes

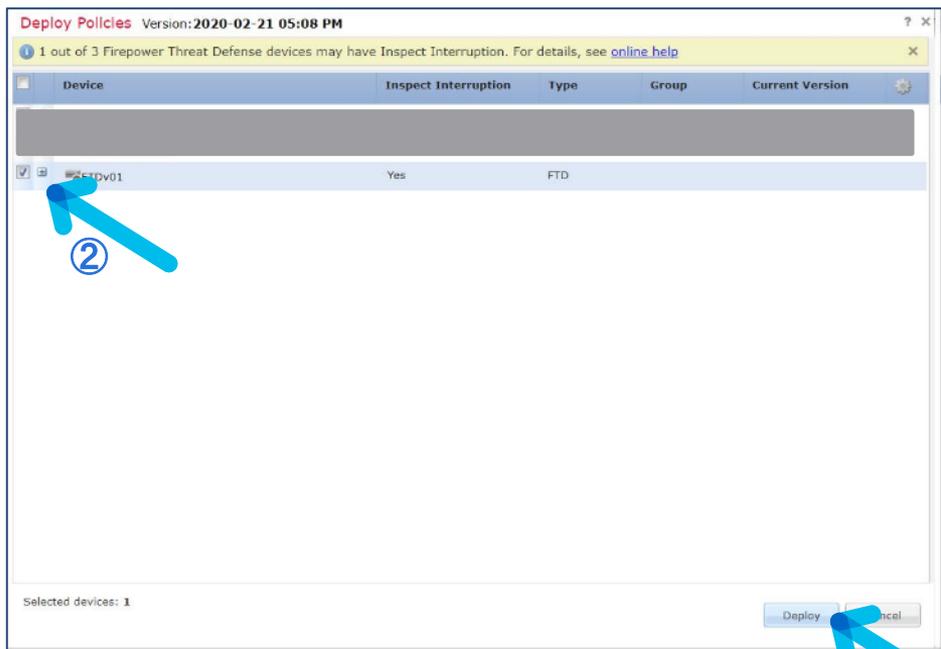
- ① Policy Informationをクリック
- ② Commit Changesをクリック

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

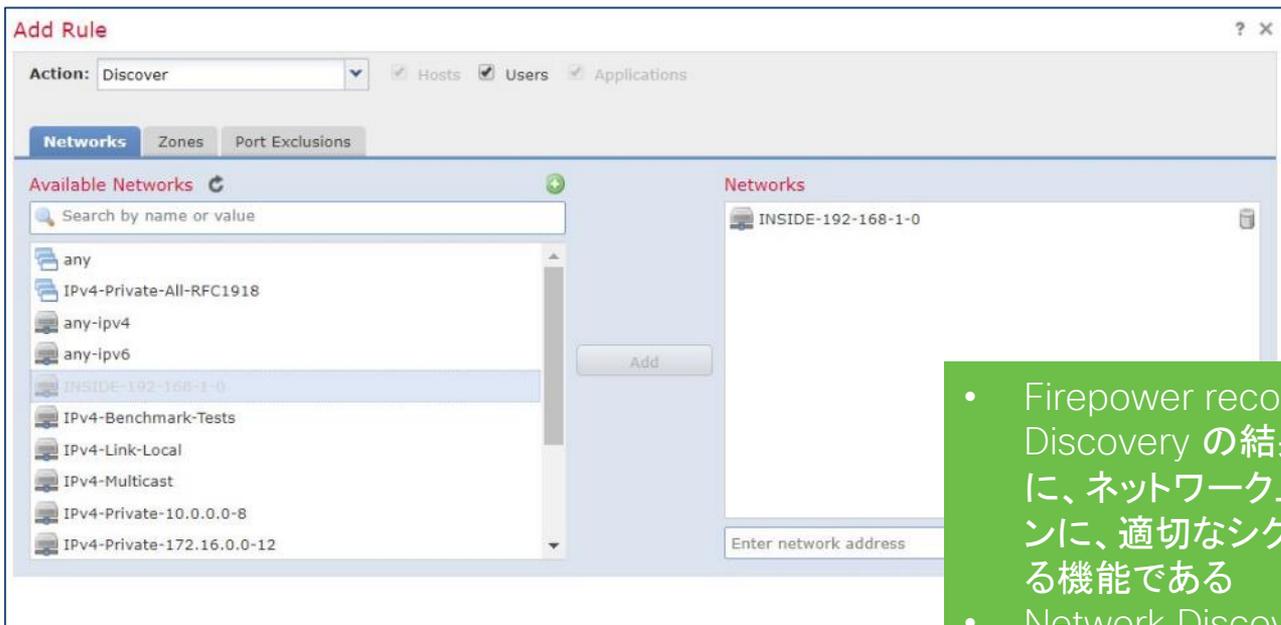


- ① Deployをクリック
- ② 変更された設定を確認の上、Deploy対象機器にチェックを入れる
- ③ Deployをクリック

- 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】

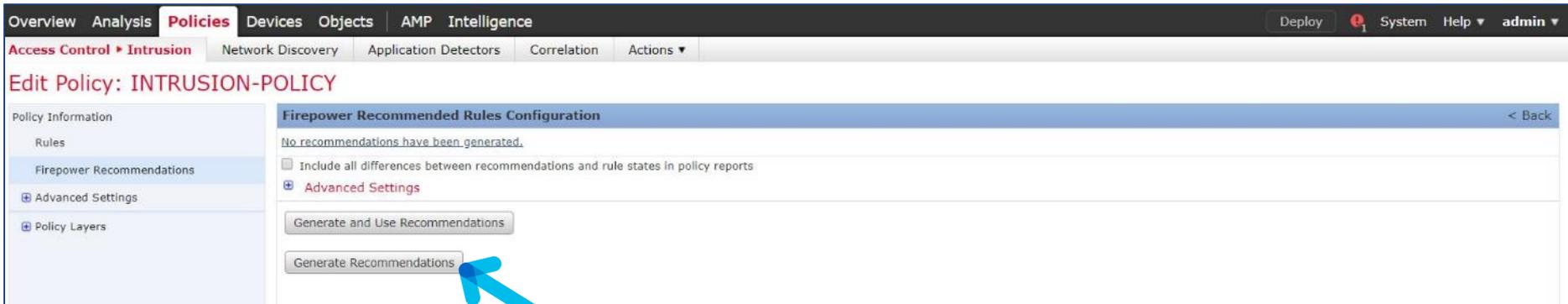
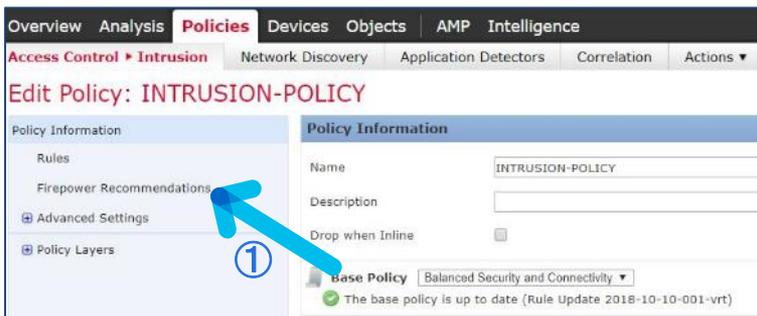
Firepower recommendation によるルールの最適化



- 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

The screenshot shows the Cisco Firepower Management Center interface. The top navigation bar includes "Overview", "Analysis", "Policies", "Devices", "Objects", "AMP", and "Intelligence". The "Policies" tab is active. Below the navigation bar, there are tabs for "Access Control", "Intrusion", "Network Discovery", "Application Detectors", "Correlation", and "Actions". The main content area is titled "Edit Policy: test-ips-ngips". On the left, there is a sidebar with "Policy Information", "Rules", "Firepower Recommendations", "Advanced Settings", and "Policy Layers". The main content area shows the "Firepower Recommended Rules Configuration" section. It displays a summary: "Firepower changed 19795 rule states for 70 hosts". Below this, there are three items: "Set 162 rules to generate events" (green arrow), "Set 6640 rules to drop and generate events" (red X), and "Set 12993 rules to disabled" (green arrow). There are "View Recommended Changes" and "View" buttons for each item. Below the summary, there is a message: "Policy is using the recommendations. Click to change recommendations." and "Last generated: 2020 Feb 21 16:23:20". There are also checkboxes for "Include all differences between recommendations and rule states in policy reports" and "Advanced Settings". At the bottom, there are two buttons: "Do Not Use Recommendations" and "Update Recommendations".

8. Malware & File Policyの設定

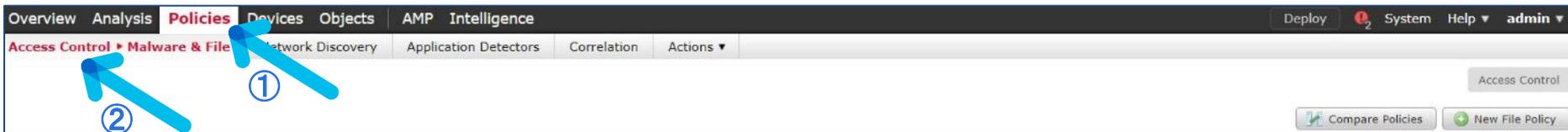
File Policyの概要

- 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 / ログイングよりも優先される
 - 例) ブロックをするルールとマルウェアインスペクションルールの二つのが同じファイルに対して有効な場合、このファイルはブロックされるだけとなり、マルウェアインスペクションは行われない

ステップ1: File Policyの作成

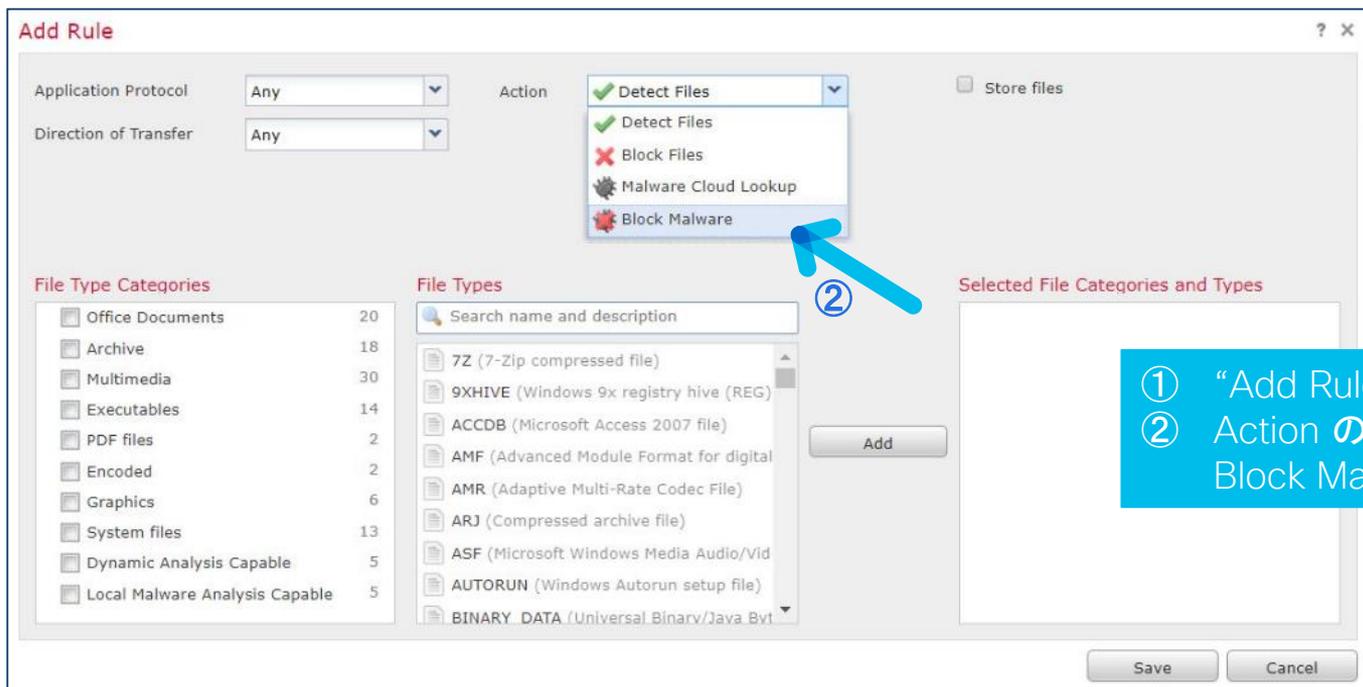


The 'New File Policy' dialog box is shown. It has a title bar with a question mark and a close button. The 'Name' field contains the text 'FILE-POLICY'. The 'Description' field is empty. At the bottom, there are 'Save' and 'Cancel' buttons. A blue arrow labeled '4' points to the 'Name' field, and another blue arrow labeled '5' points to the 'Save' button.

- 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 “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

Add Rule

Application Protocol: Any

Direction of Transfer: Any

Action: Block Malware

Store Files:

- Malware
- Unknown
- Clean
- Custom

File Type Categories:

<input type="checkbox"/> Office Documents	15
<input type="checkbox"/> Archive	17
<input type="checkbox"/> Multimedia	2
<input type="checkbox"/> Executables	9
<input type="checkbox"/> PDF files	1
<input type="checkbox"/> Encoded	0
<input type="checkbox"/> Graphics	0
<input type="checkbox"/> System files	2
<input type="checkbox"/> Dynamic Analysis Capable	5
<input type="checkbox"/> Local Malware Analysis Capable	5

File Types:

- 7Z (7-Zip compressed file)
- ACCDB (Microsoft Access 2007 file)
- ARJ (Compressed archive file)
- BINARY_DATA (Universal Binary/Java Bytecode)
- BINHEX (Macintosh BinHex 4 Compressed archive)
- BZ (bzip2 compressed archive)
- CPIO_CRC (Archive created with the cpio utility)
- CPIO_NEWC (Archive created with the cpio utility)
- CPIO_ODC (Archive created with the cpio utility)

Selected File Categories and Types:

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)。この状態では接続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

Add Rule ? x

Application Protocol: Any
Direction of Transfer: Any
Action: Block Malware

Spero Analysis for MSEXE
 Dynamic Analysis
 Capacity Handling ⓘ
 Local Malware Analysis
 Reset Connection

File Type Categories

<input checked="" type="checkbox"/> Office Documents	15
<input checked="" type="checkbox"/> Archive	17
<input checked="" type="checkbox"/> Multimedia	2
<input checked="" type="checkbox"/> Executables	9
<input checked="" type="checkbox"/> PDF files	1
<input checked="" type="checkbox"/> Encoded	0
<input checked="" type="checkbox"/> Graphics	0
<input checked="" type="checkbox"/> System files	2
<input checked="" type="checkbox"/> Dynamic Analysis Capable	5
<input checked="" type="checkbox"/> Local Malware Analysis Capable	5

File Types

Search name and description

- All types in selected Categories
- 7Z (7-Zip compressed file)
- ACCDB (Microsoft Access 2007 file)
- ARJ (Compressed archive file)
- BINARY_DATA (Universal Binary/Java Bytecode)
- BINHEX (Macintosh BinHex 4 Compressed archive)
- BZ (bzip2 compressed archive)
- CPIO_CRC (Archive created with the cpio command)
- CPIO_NEWC (Archive created with the cpio command)

Selected File Categories and Types

- Category: Local Malware Analysis Capable
- Category: Dynamic Analysis Capable
- Category: System files
- Category: Graphics
- Category: Encoded
- Category: PDF files
- Category: Executables
- Category: Multimedia
- Category: Archive
- Category: Office Documents

Save Cancel

- 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

Add Rule

Application Protocol: Any

Direction of Transfer: Any

Action: Block Malware

Spero Analysis for MSEXE

Dynamic Analysis

Capacity Handling ⓘ

Local Malware Analysis

Reset Connection

Store Files

Malware

Unknown

Clean

Custom

File Type Categories

<input checked="" type="checkbox"/> Office Documents	15
<input checked="" type="checkbox"/> Archive	17
<input checked="" type="checkbox"/> Multimedia	2
<input checked="" type="checkbox"/> Executables	9
<input checked="" type="checkbox"/> PDF files	1
<input checked="" type="checkbox"/> Encoded	0
<input checked="" type="checkbox"/> Graphics	0
<input checked="" type="checkbox"/> System files	2
<input checked="" type="checkbox"/> Dynamic Analysis Capable	5
<input checked="" type="checkbox"/> Local Malware Analysis Capable	5

File Types

Search name and description

All types in selected Categories

- 7Z (7-Zip compressed file)
- ACCDB (Microsoft Access 2007 file)
- ARJ (Compressed archive file)
- BINARY_DATA (Universal Binary/Java Bytecode)
- BINHEX (Macintosh BinHex 4 Compressed archive)
- BZ (bzip2 compressed archive)
- CPIO_CRC (Archive created with the cpio utility)
- CPIO_NEWC (Archive created with the cpio utility)

Selected File Categories and Types

- Category: Local Malware Analysis Capable
- Category: Dynamic Analysis Capable
- Category: System files
- Category: Graphics
- Category: Encoded
- Category: PDF files
- Category: Executables

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



The screenshot shows the Cisco AMP console interface for configuring a File Rule. The breadcrumb navigation is "Access Control > Malware & File". The rule name is "test-file". The "Rules" tab is active, and the "Advanced" view is selected. A table lists the rule configuration:

File Types	Application Protocol	Direction	Action
<ul style="list-style-type: none">Category: Local Malware Analysis CapableCategory: Dynamic Analysis CapableCategory: System filesCategory: Graphics (6 more...)	Any	Any	<ul style="list-style-type: none">Block Malware with ResetSpero AnalysisLocal Malware AnalysisStore files of disposition: Malware

An "Add Rule" button with a green plus icon is located in the top right corner of the table area. A blue arrow points to this button, which is also marked with a circled "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

Add Rule

Application Protocol: Any

Direction of Transfer: Any

Action: Block Malware

- Spero Analysis for MSEXE
- Dynamic Analysis
- Capacity Handling
- Local Malware Analysis
- Reset Connection

Store Files

- Malware
- Unknown
- Clean
- Custom

File Type Categories

<input type="checkbox"/> Office Documents	15
<input type="checkbox"/> Archive	17
<input type="checkbox"/> Multimedia	2
<input type="checkbox"/> Executables	9
<input type="checkbox"/> PDF files	1
<input type="checkbox"/> Encoded	0
<input type="checkbox"/> Graphics	0
<input type="checkbox"/> System files	2
<input checked="" type="checkbox"/> Dynamic Analysis Capable	5
<input type="checkbox"/> Local Malware Analysis Capable	5

File Types

Search name and description

- All types in selected Categories
- MSEXE (Windows/DOS executable file)
- MSOLE2 (Microsoft Object Linking and Embe
- NEW_OFFICE (Microsoft Office Open XML Fo
- PDF (PDF file)
- RTF (Rich text format word processing file)

Selected File Categories and Types

Category: Dynamic Analysis Capable

⑤ Add

⑥ Save Cancel

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

① 今回は設定対象としないが、Advancedをクリックすることで下記の追加設定が可能

①

FILE-POLICY

Enter Description

Rules **Advanced**

You have unsaved changes Save Cancel

Revert to Defaults

General

- First Time File Analysis
- Enable Custom Detection List
- Enable Clean List
- Override AMP Cloud Disposition Based upon Threat Score: Disabled

Archive File Inspection

- Inspect Archives
- Block Encrypted Archives
- Block Uninspectable Archives
- Max Archive Depth: 2

説明:

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

ステップ4: Advancedタブの確認とFile Policy保存②



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

Access Control Malware & File Network Discovery Application Detectors Correlation Actions

test-file

Enter Description

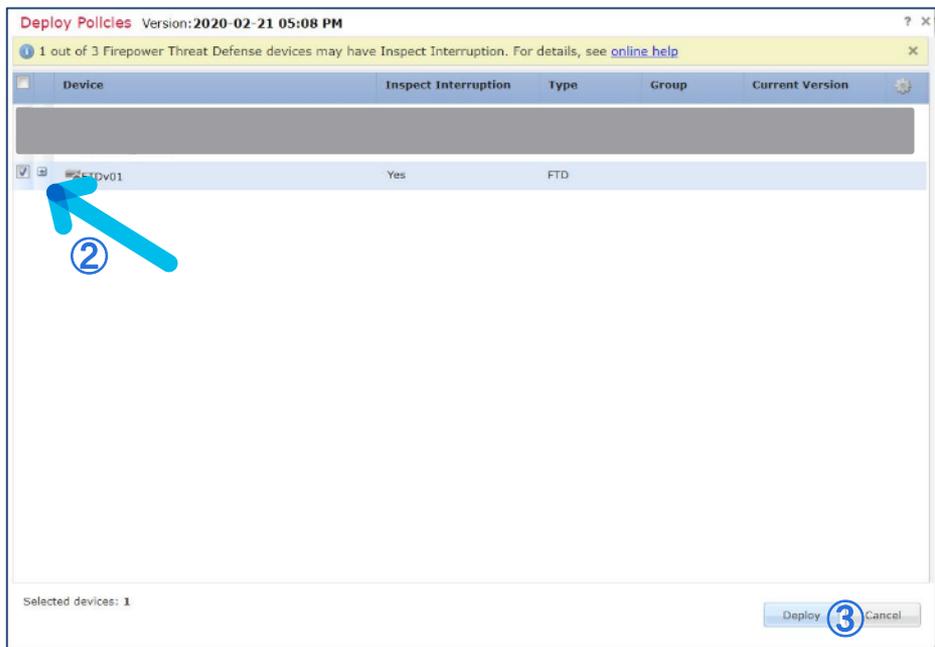
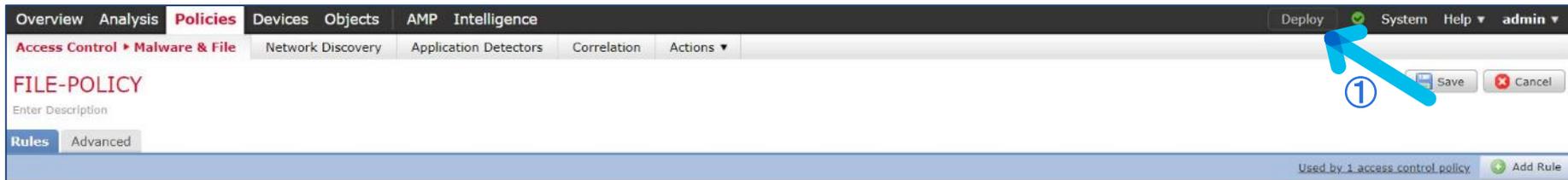
Rules Advanced

You have unsaved changes Save Cancel

Used by 1 access control policy Add Rule

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)



The screenshot shows the Cisco AMP Threat Grid web interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'AMP' tab is active, and the 'Dynamic Analysis Connections' sub-tab is selected. A blue arrow points to this sub-tab, with a circled '1' next to it. Below the navigation, there is a table with columns for 'Cloud Name', 'Host', 'Purpose', and 'Actions'. The first row shows 'Cisco Sandbox API, US Cloud' as the cloud name, 'fmc.api.threatgrid.com' as the host, and 'File Submissions, Public Report Lookups' as the purpose. An 'Add New Connection' button is visible in the top right corner.

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

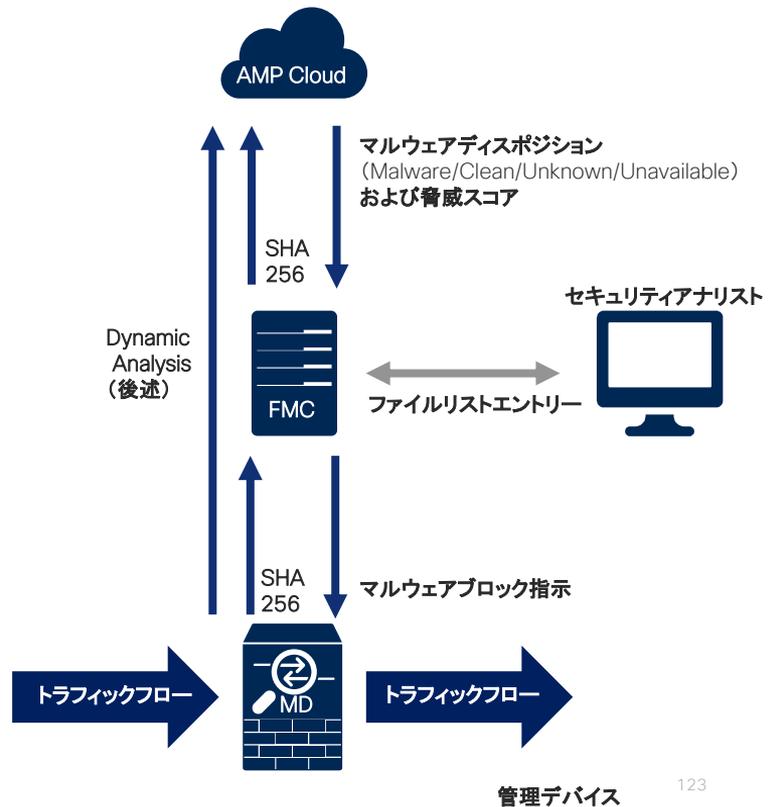
- ① Dynamic Analysis Connectionsをクリックし、AMP Threat Grid設定を確認
※現時点でThread Gridクラウド環境は、APJCIにはない。

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)

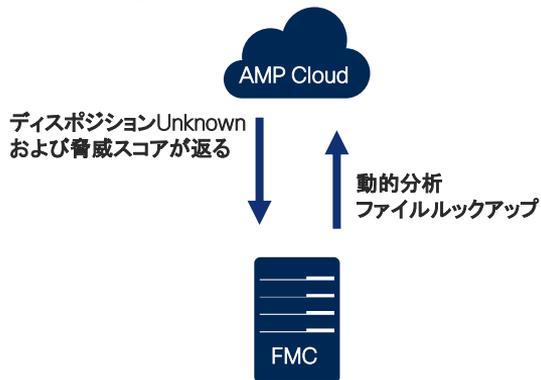
101010
100101
001001



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)



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

分析の
順序

Spero Analysis

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

ローカルマルウェア分析(Local Malware Analysis)

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

動的分析(Dynamic Analysis)

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

参考: マルウェアのクラウドリコール

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



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

世界最大規模の脅威検出ネットワーク

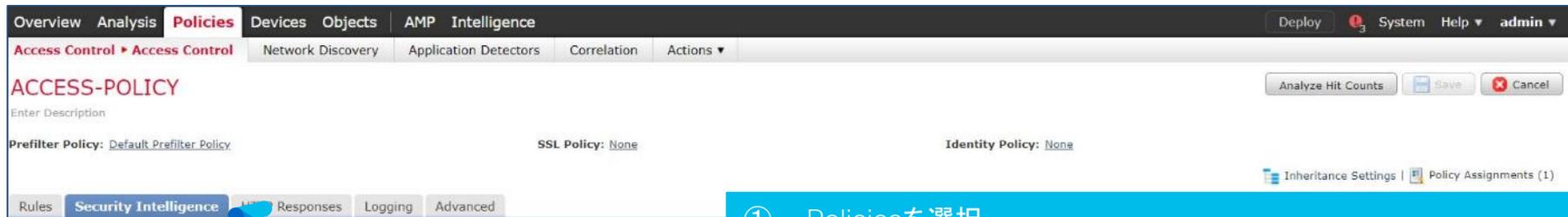
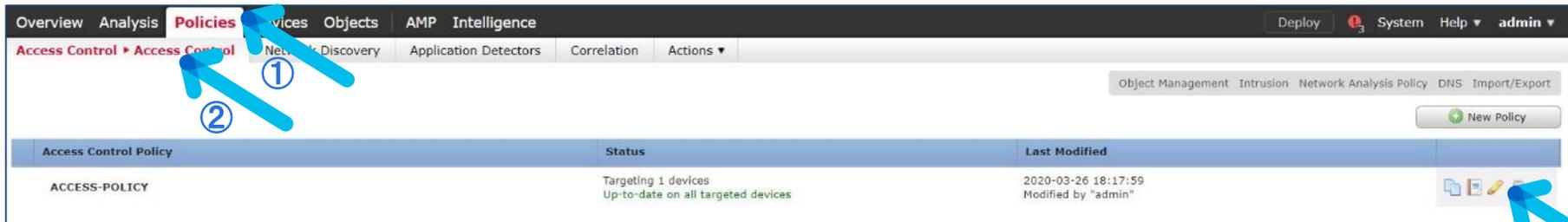
Cisco Security Intelligence Operations (SIO) は、全世界のセキュリティ情報を収集し、脅威や脆弱性に関する情報や分析を提供しています。

[SIO にアクセス](#)



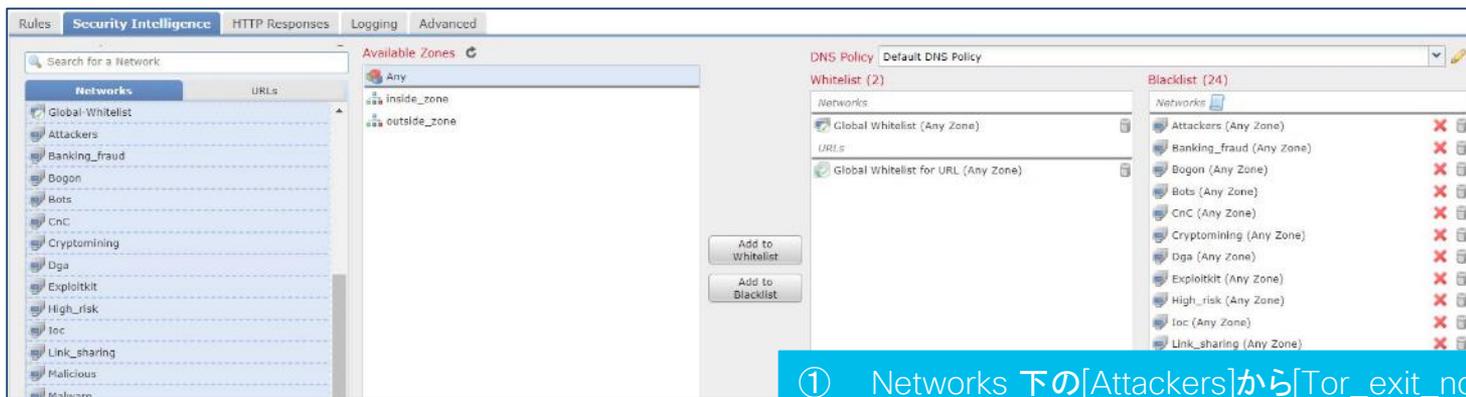
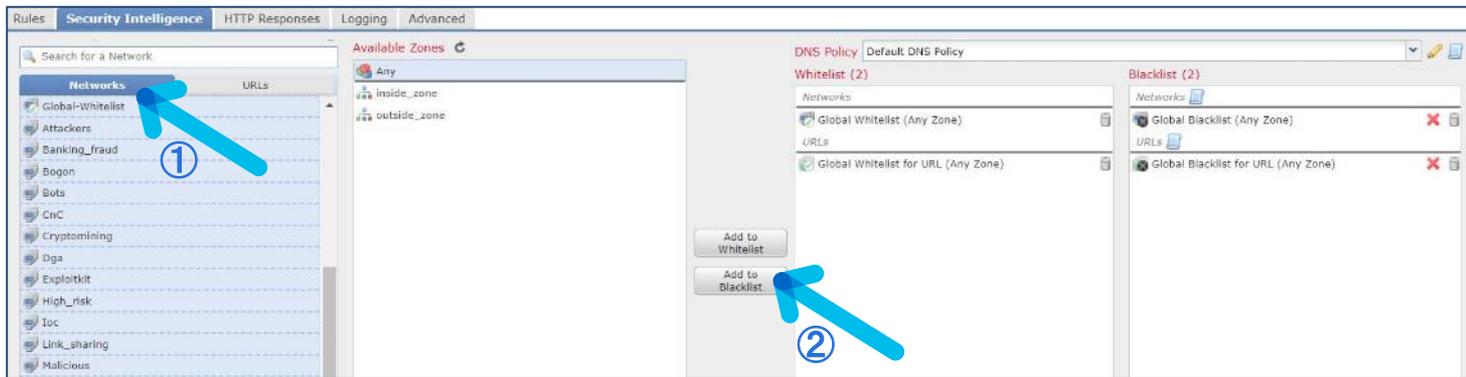
ステップ 1: Security Intelligence の設定

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



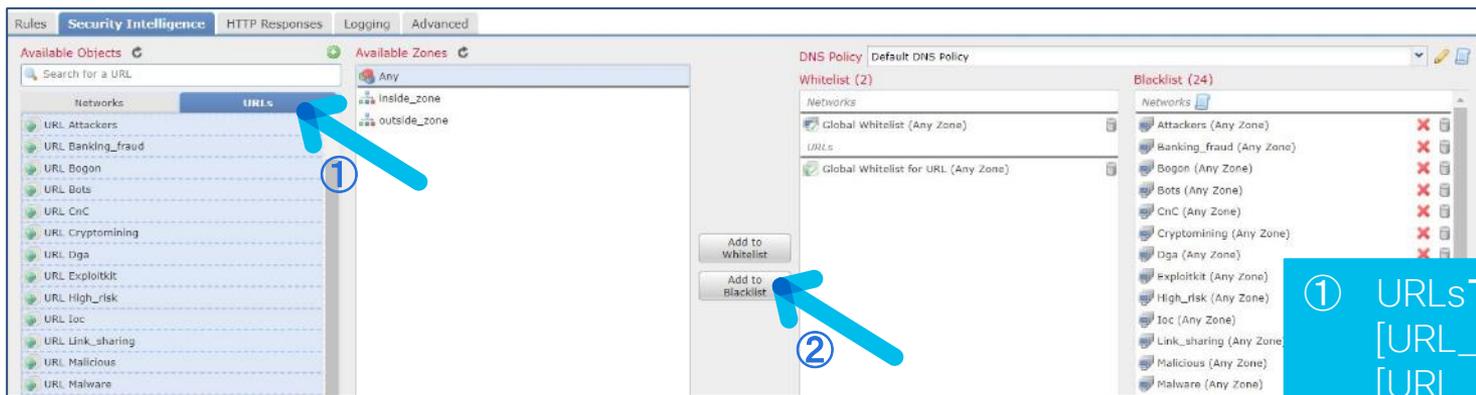
- ① Policiesを選択
- ② Access Controlを選択
- ③ 設定対象のAccess Control Policy(ここでは1章で作成済みの“ACCESS-POLICY”とする)の右側の鉛筆マークを選択
- ④ Security Intelligence を選択

ステップ 1: Security Intelligence の設定 Network

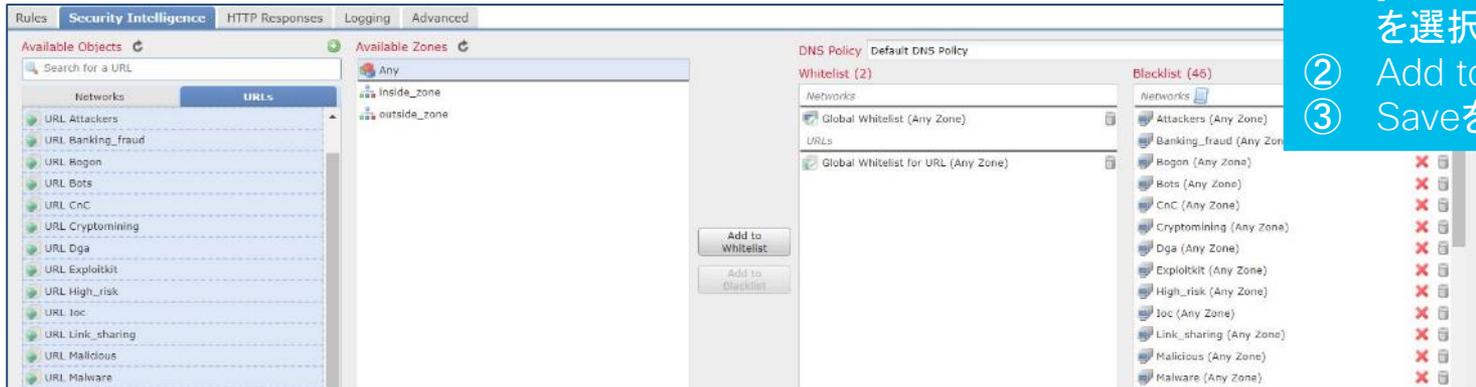


- ① Networks 下の[Attackers]から[Tor_exit_node]までを選択
- ② Add to Blacklist をクリック

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



ACCESS-POLICY

Enter Description

Prefilter Policy: Default Prefilter Policy

SSL Policy: None

Identity Policy: None

You have unsaved changes

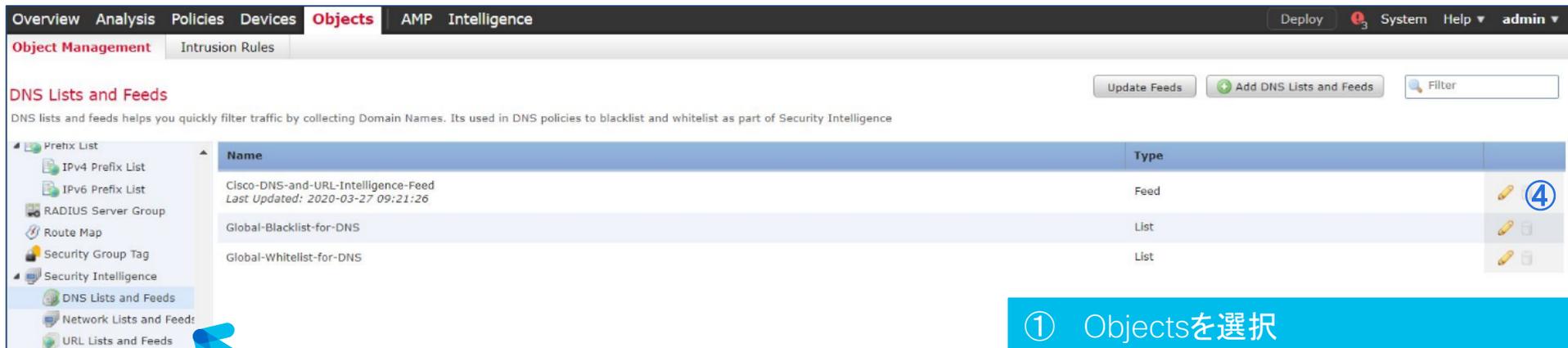
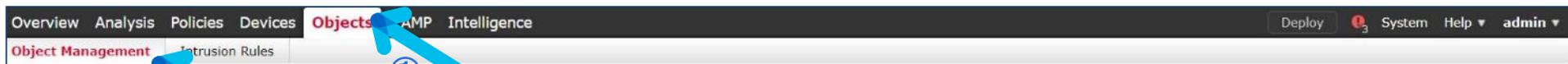
Analyze Hit Counts

Save

Cancel

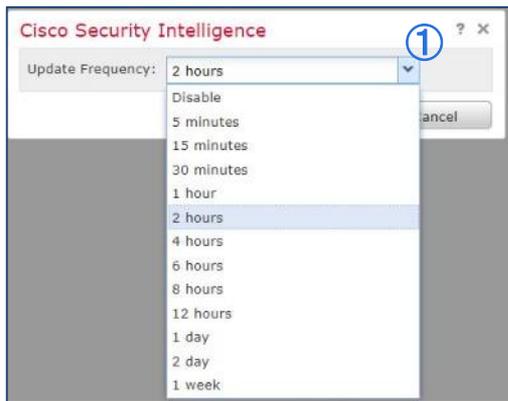
③

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

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

Object Management Intrusion Rules

DNS Lists and Feeds

Update Feeds + Add DNS Lists and Feeds

DNS lists and feeds helps you quickly filter traffic by collecting Domain Names. Its used in DNS policies to blacklist and whitelist as part of Security Intelligence

Name	Type	
Cisco-DNS-and-URL-Intelligence-Feed <i>Last Updated: 2020-03-27 09:21:26</i>	Feed	
Global-Blacklist-for-DNS	List	
Global-Whitelist-for-DNS	List	

Left sidebar menu: Prelix List, IPv4 Prefix List, IPv6 Prefix List, RADIUS Server Group, Route Map, Security Group Tag, Security Intelligence, **DNS Lists and Feeds**, Network Lists and Feeds, URL Lists and Feeds

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

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

Access Control Access Control Network Discovery Application Detectors Correlation Actions

Object Management Intrusion Network Analysis Policy DNS Import/Export

New Policy

Access Control Policy	Status	Last Modified	
ACCESS-POLICY	Targeting 1 devices Up-to-date on all targeted devices	2020-03-26 18:17:59 Modified by "admin"	

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

Access Control Access Control Network Discovery Application Detectors Correlation Actions

ACCESS-POLICY Analyze Hit Counts Save Cancel

Enter Description

Prefilter Policy: Default Prefilter Policy SSL Policy: None Identity Policy: None

Inheritance Settings Policy Assignments (1)

Rules Security Intelligence HTTP Responses Logging Advanced

Show Rule Conflicts Add Category Add Rule

Name	Source Zones	Dest Zones	Source Net...	Dest Netwo...	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	ISE/SGT At...	Ac...
Mandatory - ACCESS-POLICY (-)												

- 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

The screenshot shows the 'Add Rule' configuration window. The 'Name' field contains 'CATCH-ALL'. The 'Action' dropdown is set to 'Allow'. The 'Insert' dropdown is set to 'into Default'. The 'Inspection' tab is selected. The 'Intrusion Policy' dropdown is set to 'INTRUSION-POLICY'. The 'File Policy' dropdown is set to 'FILE-POLICY'. The 'Variable Set' dropdown is set to 'Default Set'. The 'Enabled' checkbox is checked. The 'Zones', 'Networks', 'VLAN Tags', 'Users', 'Applications', 'Ports', 'URLs', and 'SGT/ISE Attributes' tabs are visible. The 'Inspection' and 'Logging' tabs are also visible.

- 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 [FILE-POLICY]を選択

ステップ 2: Access Rule の設定③

Editing Rule - CATCH-ALL

Name: CATCH-ALL Enabled [Move](#)

Action: Allow

Zones Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes **Inspection** **Logging** Comments

Log at Beginning of Connection

Log at End of Connection

File Events:

Log Files

Send Connection Events to:

Event Viewer

Syslog Server (Using default syslog configuration in Access Control Logging) [Show Overrides](#)

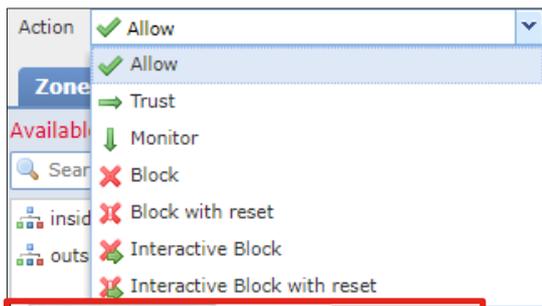
SNMP Trap

4 Add Cancel

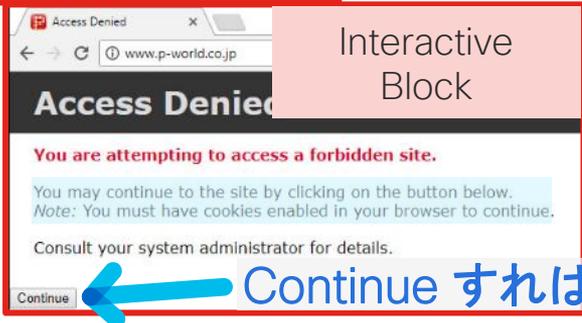
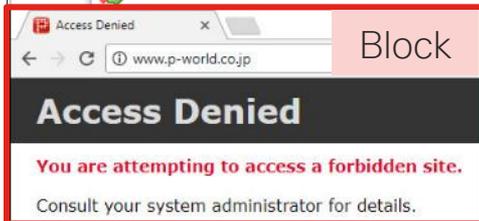
※Loggingの負荷が高い場合には②を省くことを推奨

- 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

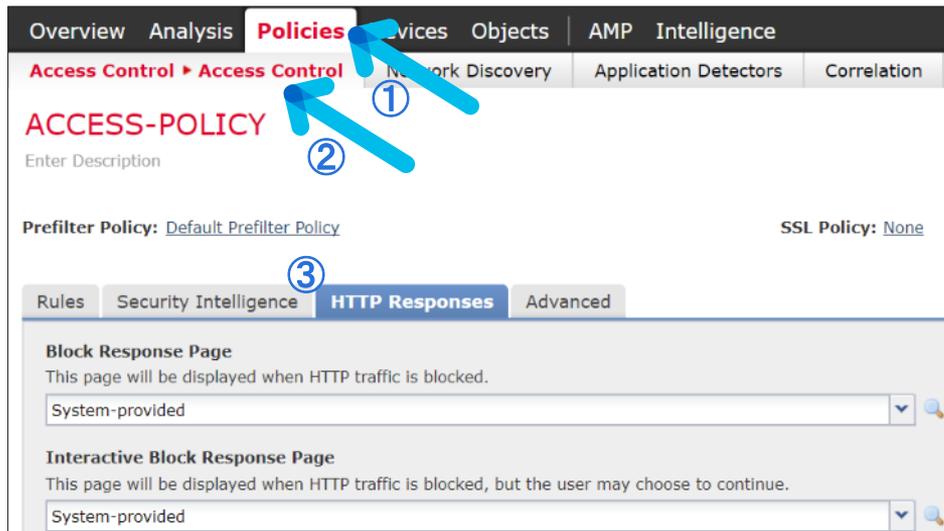


- FTD で使用できる Action は全 7 種
 - Allow: パケットを信頼せずに許可し、追加でIPSやAMPのチェックを実施することが可能
 - Trust: パケットを信頼して許可。IPSやAMPのチェックは不可
 - Monitor: ログを取るためだけに使用。トラフィックは次のルールに転送
 - Block: パケットを破棄
 - Block w/ reset: パケットを破棄すると同時に、送信元に対し、TCP RSTパケットを送信し、通信を即遮断
 - Interactive Block: ブロックが推奨されるユーザアクションに対し警告を行うが、ユーザの判断で通信し続ける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

Access Denied

禁止されているサイトへのアクセスを試みようとしています。

詳細についてはシステム管理者へお問い合わせください。

② Save

- 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

The screenshot shows the Cisco AMP for Networks configuration interface. The top navigation bar includes 'System' (selected) and 'admin'. The sub-navigation bar includes 'Integration' (selected). The main content area shows the 'URL Filtering' configuration page. The 'URL Filtering' section has a toggle switch turned on. The 'AMP for Networks' section shows the last local malware detection update. The 'Cisco Cloud' section has a toggle switch turned off.

- 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カテゴリーのロギングを行うRuleを追加

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

Access Control Access Control Network Discovery Application Detectors Correlation Actions

Object Management Intrusion Network Analysis Policy DNS Import/Export

New Policy

Access Control Policy	Status	Last Modified	
ACCESS-POLICY	Targeting 1 devices Up-to-date on all targeted devices	2020-03-26 18:17:59 Modified by "admin"	

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

Access Control Access Control Network Discovery Application Detectors Correlation Actions

ACCESS-POLICY Analyze Hit Counts Save Cancel

Enter Description

Prefilter Policy: Default Prefilter Policy SSL Policy: None Identity Policy: None

Inheritance Settings Policy Assignments (1)

Rules Security Intelligence HTTP Responses Logging Advanced

Show Rule Conflicts Add Category Add Rule

Name	Source Zones	Dest Zones	Source Net...	Dest Netwo...	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	ISE/SGT At...	Ac...
Mandatory - ACCESS-POLICY (-)												

- 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

Add Rule

Name: URL-MONITOR ① Enabled

Action: Monitor ②

Insert: above rule ③

Zones Networks ② VLAN Tags Users Applications Ports **URLs** SGT/ISE Attributes Inspection Logging Comments

Categories and URLs

Search for a category

Category	URLs
Any (Except Uncategorized)	
Uncategorized	
Abortion	
Abused Drugs	
Adult and Pornography	
Alcohol and Tobacco	
Auctions	
Bot Nets	
Business and Economy	

Reputations

- Any
- 5 - Well Known
- 4 - Benign sites
- 3 - Benign sites with security risks
- 2 - Suspicious sites
- 1 - High Risk

Selected URLs (0)

any

Add to Rule

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

The screenshot shows the 'Add Rule' configuration window for a URL Category Monitor. The rule name is 'URL-MONITOR', it is enabled, and the action is 'Monitor'. The 'URLs' tab is selected in the top navigation bar. In the 'Categories and URLs' section, 'Any (Except Uncategorized)' is selected. In the 'Reputations' section, '5 - Well Known' is selected. The 'Add to Rule' button is highlighted with a blue arrow and callout 4. The 'Add' button at the bottom right is highlighted with a blue arrow and callout 5. Other callouts include 1 pointing to the 'URLs' tab, 2 pointing to 'Any (Except Uncategorized)', and 3 pointing to '5 - Well Known'.

※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

Overview Analysis **Policies** Devices Objects AMP Intelligence

Access Control Access Control Network Discovery Application Detectors Correlation Actions

ACCESS-POLICY

You have unsaved changes Analyze Hit Count Save Cancel

Enter Description

Prefilter Policy: Default Prefilter Policy SSL Policy: None Identity Policy: None

Inheritance Settings Policy Assignments (1)

Rules Security Intelligence HTTP Responses Logging Advanced

Filter by Device Show Rule Conflicts Add Category Add Rule Search Rules

#	Name	Source Zones	Dest Zones	Source Net...	Dest Netwo...	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	ISE/SCT At...	Action
Mandatory ACCESS-POLICY (-)													
There are no rules in this section. Add Rule or Add Category													
Default ACCESS-POLICY (1-2)													
Deploy Policies Version: 2020 02 21 05:08 PM													
1 out of 3 Firepower Threat Defense devices may have Inspect Interruption. For details, see online help													
Device	Inspect Interruption	Type	Group	Current Version									
<input checked="" type="checkbox"/>													
FTDv01	Yes	FTD											

Selected devices: 1

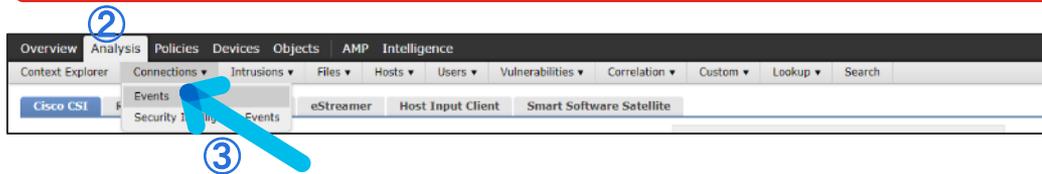
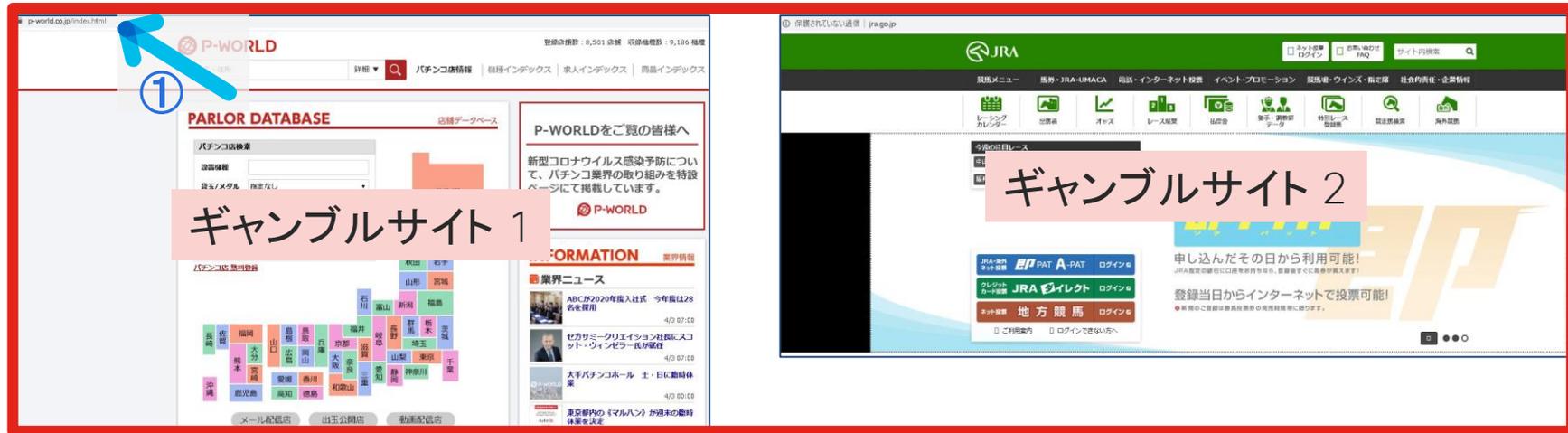
Deploy Cancel

- 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



Connection Events (switch workflow)
Connections with Application Details > Table View of Connection Events
No Search Constraints (Edit Search) ④

- 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

(unnamed search) Private Save Save As New Search

Referenced Host	<input type="text"/>	example.com
User Agent	<input type="text"/>	Mozilla/5.0, Firefox, Chrome
HTTP Referrer	<input type="text"/>	http://example.com/index.html
URL		
URL	<input type="text"/>	http://example.com/index.html
URL Category	<input type="text" value="Gambling"/>	Shopping, Travel
URL Reputation	<input type="text"/>	Well known, High risk

- 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

Connection Events (switch workflow) 2020-04-13 09:42:06 - 2020-04-13 09:59:02

[Connections with Application Details](#) > [Table View of Connection Events](#)

▶ Search Constraints (Edit Search Save Search)

Jump to... ▼

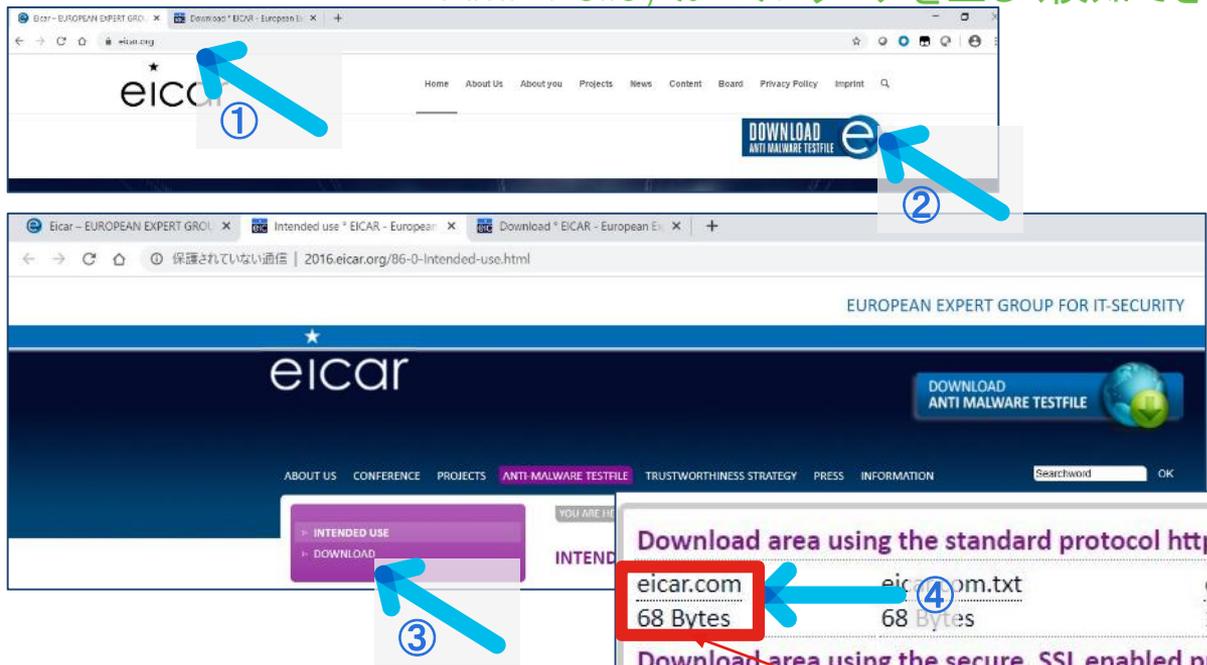
First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Web Application	URL	URL Category	URL Res
2020-04-13 09:41:39	2020-04-13 09:41:39	Allow		192.168.1.101	JPN	210.160.2.77	JPN	inside_zone	outside_zone	52085 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	http://thorse.ra.gg.jp/bca/r_t_top.js	Gambling	Well
2020-04-13 09:41:39	2020-04-13 09:41:39	Allow		192.168.1.101	JPN	210.160.2.77	JPN	inside_zone	outside_zone	52086 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	http://thorse.ra.gg.jp/bca/eq/1586738500041/0/71...	Gambling	Well
2020-04-13 09:41:39	2020-04-13 09:41:39	Allow		192.168.1.101	JPN	210.160.2.77	JPN	inside_zone	outside_zone	52086 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	http://thorse.ra.gg.jp/bca/eq/1586738500041/0/71...	Gambling	Well
2020-04-13 09:41:39	2020-04-13 09:41:39	Allow		192.168.1.101	JPN	210.160.2.77	JPN	inside_zone	outside_zone	52085 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	http://thorse.ra.gg.jp/bca/r_t_top.js	Gambling	Well
2020-04-13 09:41:38	2020-04-13 09:41:41	Allow		192.168.1.101	JPN	210.149.135.21	JPN	inside_zone	outside_zone	52079 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	http://www.ra.gg.jp_top/ans/mno/btn_facebook.png	Gambling	Well
2020-04-13 09:41:38	2020-04-13 09:41:41	Allow		192.168.1.101	JPN	210.149.135.21	JPN	inside_zone	outside_zone	52078 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	http://www.ra.gg.jp_top/header/img/btn_banner_e...	Gambling	Well
2020-04-13 09:41:38	2020-04-13 09:41:41	Allow		192.168.1.101	JPN	210.149.135.21	JPN	inside_zone	outside_zone	52081 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	http://www.ra.gg.jp_top/fonts/fontawesome-webfon...	Gambling	Well
2020-04-13 09:41:38	2020-04-12 09:41:01	Allow		192.168.1.101	JPN	210.149.135.21	JPN	inside_zone	outside_zone	52080 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	http://www.ra.gg.jp_top/ans/mno/btn_instagram.jp...	Gambling	Well
2020-04-13 09:41:38	2020-04-13 09:41:38	Allow		192.168.1.101	JPN	210.149.135.21	JPN	inside_zone	outside_zone	52081 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	http://www.ra.gg.jp_top/css/font-awesome.css	Gambling	Well
2020-04-13 09:41:38	2020-04-13 09:41:38	Allow		192.168.1.101	JPN	210.149.135.21	JPN	inside_zone	outside_zone	52078 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	http://www.ra.gg.jp_top/css/custom.css?version=...	Gambling	Well
2020-04-13 09:41:38	2020-04-13 09:41:38	Allow		192.168.1.101	JPN	210.149.135.21	JPN	inside_zone	outside_zone	52079 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	http://www.ra.gg.jp/common/js/common2.js	Gambling	Well
2020-04-13 09:41:38	2020-04-13 09:41:38	Allow		192.168.1.101	JPN	210.149.135.21	JPN	inside_zone	outside_zone	52080 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	http://www.ra.gg.jp_top/css/top.css?version=201...	Gambling	Well
2020-04-13 09:41:37	2020-04-13 09:41:41	Allow		192.168.1.101	JPN	210.149.135.21	JPN	inside_zone	outside_zone	52076 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	http://www.ra.gg.jp_top/ans/mno/btn_youtube.jp...	Gambling	Well
2020-04-13 09:41:37	2020-04-13 09:41:37	Allow		192.168.1.101	JPN	210.149.135.21	JPN	inside_zone	outside_zone	52075 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	http://www.ra.gg.jp_top/img/btn_nageton.png	Gambling	Well
2020-04-13 09:41:37	2020-04-13 09:41:37	Allow		192.168.1.101	JPN	210.149.135.21	JPN	inside_zone	outside_zone	52075 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	http://www.ra.gg.jp/	Gambling	Well
2020-04-13 09:41:37	2020-04-13 09:41:37	Allow		192.168.1.101	JPN	210.149.135.21	JPN	inside_zone	outside_zone	52076 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	http://www.ra.gg.jp_top/css/fonts.css	Gambling	Well
2020-04-13 09:41:21	2020-04-13 09:41:25	Allow		192.168.1.101	JPN	202.214.243.183	JPN	inside_zone	outside_zone	52045 / tcp	443 (https) / tcp	HTTP	Chrome	Squid	https://www.e-world.co.jp/img/index/iconAppSw...	Gambling	Well
2020-04-13 09:41:21	2020-04-13 09:41:35	Allow		192.168.1.101	JPN	202.214.243.183	JPN	inside_zone	outside_zone	52046 / tcp	443 (https) / tcp	HTTP	Chrome	Chrome	https://www.e-world.co.jp/img/index/iconCaruseAr...	Gambling	Well
2020-04-13 09:41:21	2020-04-13 09:41:35	Allow		192.168.1.101	JPN	202.214.243.183	JPN	inside_zone	outside_zone	52047 / tcp	443 (https) / tcp	HTTP	Chrome	Squid	https://www.e-world.co.jp/img/index/iconCaruseAr...	Gambling	Well
2020-04-13 09:41:21	2020-04-13 09:41:35	Allow		192.168.1.101	JPN	202.214.243.183	JPN	inside_zone	outside_zone	52044 / tcp	443 (https) / tcp	HTTP	Chrome	Squid	https://www.e-world.co.jp/img/index/iconAppTwitter...	Gambling	Well
2020-04-13 09:41:21	2020-04-13 09:41:35	Allow		192.168.1.101	JPN	202.214.243.183	JPN	inside_zone	outside_zone	52042 / tcp	443 (https) / tcp	HTTP	Chrome	Squid	https://www.e-world.co.jp/maos/sal/e-world.gif	Gambling	Well
2020-04-13 09:41:21	2020-04-13 09:41:35	Allow		192.168.1.101	JPN	202.214.243.183	JPN	inside_zone	outside_zone	52043 / tcp	443 (https) / tcp	HTTP	Chrome	Squid	https://www.e-world.co.jp/maos/index?20200320	Gambling	Well
2020-04-13 09:41:21	2020-04-13 09:41:32	Allow		192.168.1.101	JPN	99.84.133.31	JPN	inside_zone	outside_zone	52048 / tcp	443 (https) / tcp	HTTP	Chrome	Web Browsing	https://dn.e-world.co.jp/maker/sites/site_7.png	Gambling	Well
2020-04-13 09:41:21	2020-04-13 09:41:32	Allow		192.168.1.101	JPN	99.84.133.31	JPN	inside_zone	outside_zone	52053 / tcp	443 (https) / tcp	HTTP	Chrome	Web Browsing	https://dn.e-world.co.jp/news/greenbank/2289/273...	Gambling	Well

① ギャンブルサイトがURL CategoryでGamblingへカテゴリ化されていることを確認



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



- 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

Download area using the standard protocol http

eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes
-----------------------	---------------------------	----------------------------	----------------------------

Download area using the secure, SSL enabled protocol https

eicar.com	eicar.com.txt	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes
-----------	---------------	----------------------------	----------------------------

テスト用マルウェアファイル

ステップ 7: AMP (File Policy) のテスト②

Overview Analysis Policies Devices Objects AMP Intelligence

Context Explorer **Connections** Events Sessions Files Hosts Users Correlation Advanced Search

Deploy System Help admin

Bookmark This Page Report Designer Dashboard View Bookmarks Search

2020-04-13 08:42:06 - 2020-04-13 10:05:56 Expanding

Connection Events (switch workflow) ①

Connections with Application Details Table View of Connection Events

Search Constraints (Edit Search Save Search)

Jump to...

	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Web Application	URL
↓	2020-04-13 10:00:09	2020-04-13 10:00:09	Block	File Block	192.168.1.101	DEU	213.211.198.58	DEU	inside_zone	outside_zone	52165 / tcp	80 (http) / tcp	HTTP	chrome	Web Browsing	http://2016.eicar.org/download/eicar.com
↓	2020-04-13 10:00:09		Allow		192.168.1.101	DEU	213.211.198.58	DEU	inside_zone	outside_zone	52165 / tcp	80 (http) / tcp	HTTP	chrome	Web Browsing	http://2016.eicar.org/download/eicar.com
↓	2020-04-13 09:55:08	2020-04-13 09:55:09	Block	File Block	192.168.1.101	DEU	213.211.198.58	DEU	inside_zone	outside_zone	52159 / tcp	80 (http) / tcp	HTTP	chrome	Web Browsing	http://2016.eicar.org/download/eicar.com
↓	2020-04-13 09:55:08		Allow		192.168.1.101	DEU	213.211.198.58	DEU	inside_zone	outside_zone	52159 / tcp	80 (http) / tcp	HTTP	chrome	Web Browsing	http://2016.eicar.org/download/eicar.com
↓	2020-04-13 09:54:08	2020-04-13 09:54:08	Block	File Block	192.168.1.101	DEU	213.211.198.58	DEU	inside_zone	outside_zone	52155 / tcp	80 (http) / tcp	HTTP	chrome	Web Browsing	http://2016.eicar.org/download/eicar.com
↓	2020-04-13 09:54:08		Allow		192.168.1.101	DEU	213.211.198.58	DEU	inside_zone	outside_zone	52155 / tcp	80 (http) / tcp	HTTP	chrome	Web Browsing	http://2016.eicar.org/download/eicar.com
↓	2020-04-13 09:53:37	2020-04-13 09:53:38	Block	File Block	192.168.1.101	DEU	213.211.198.58	DEU	inside_zone	outside_zone	52152 / tcp	80 (http) / tcp	HTTP	chrome	Web Browsing	http://2016.eicar.org/download/eicar.com
↓	2020-04-13 09:53:37		Allow		192.168.1.101	DEU	213.211.198.58	DEU	inside_zone	outside_zone	52152 / tcp	80 (http) / tcp	HTTP	chrome	Web Browsing	http://2016.eicar.org/download/eicar.com
↓	2020-04-13 09:53:32	2020-04-13 09:53:32	Block	File Block	192.168.1.101	DEU	213.211.198.58	DEU	inside_zone	outside_zone	52150 / tcp	80 (http) / tcp	HTTP	chrome	Web Browsing	http://2016.eicar.org/download/eicar.com
↓	2020-04-13 09:53:32		Allow		192.168.1.101	DEU	213.211.198.58	DEU	inside_zone	outside_zone	52150 / tcp	80 (http) / tcp	HTTP	chrome	Web Browsing	http://2016.eicar.org/download/eicar.com
↓	2020-04-13 09:53:31	2020-04-13 09:53:32	Block	File Block	192.168.1.101	DEU	213.211.198.58	DEU	inside_zone	outside_zone	52149 / tcp	80 (http) / tcp	HTTP	chrome	Web Browsing	http://2016.eicar.org/download/eicar.com
↓	2020-04-13 09:53:31	2020-04-13 09:53:32	Block	File Block	192.168.1.101	DEU	213.211.198.58	DEU	inside_zone	outside_zone	52148 / tcp	80 (http) / tcp	HTTP	chrome	Web Browsing	http://2016.eicar.org/download/eicar.com
↓	2020-04-13 09:53:31	2020-04-13 09:53:31	Block	File Block	192.168.1.101	DEU	213.211.198.58	DEU	inside_zone	outside_zone	52147 / tcp	80 (http) / tcp	HTTP	chrome	Web Browsing	http://2016.eicar.org/download/eicar.com

- 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

The screenshot shows the Cisco AMP console interface. The top navigation bar includes 'Overview', 'Analysis', 'Policy', 'Intelligence', 'Files', 'AMP', and 'Intelligence'. The 'Files' menu is expanded, showing 'Network File Trajectory' selected. Below the navigation bar is a search field and two tables: 'Recently Viewed Files' and 'Recent Malware'. Both tables have columns for 'Time', 'File SHA256', 'File Names', 'File Type', 'Disposition', and 'Events'. A blue arrow labeled '1' points to the 'Analysis' tab. A blue arrow labeled '2' points to the 'Files > Network File Trajectory' menu item. A blue arrow labeled '3' points to the 'File SHA256' column header in the 'Recently Viewed Files' table.

Time	File SHA256	File Names	File Type	Disposition	Events
2020-04-13 10:10:09	225a021b...f651fd0f	eicar.com	EICAR	Malware	9

Time	File SHA256	File Names	File Type	Disposition	Events
2020-04-13 10:10:09	225a021b...f651fd0f	eicar.com	EICAR	Malware	9

- 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

The screenshot displays the Cisco AMP console interface. The main view is titled "Network File Trajectory for 275a021b...f651fd0f". It shows file details for "eicar.com" (SHA256: 275a021b...f651fd0f, Size: 0.0664 KB, Type: EICAR, Category: Executables, Disposition: Malware). A blue arrow points to the "Malware" disposition with a circled "1".

Below the details is a "Trajectory" timeline showing the file's path from IP 213.211.198.58 on April 13th. A blue arrow points to the "Malware" icon on the timeline with a circled "2".

The "Events" section contains a table of file transfer events. A blue arrow points to the "Action" column, which shows "Malware Block" for all events, with a circled "2".

Time	Event Type	Sending IP	Receiving IP	User	File Name	Dispos...	Action	Protocol	Client	Web Appl...	Description
2020-04-13 09:53:31	Transfer	213.211.198.58	192.168.1.101	No Authentication Requ...	eicar.com	Malware	Malware Block	HTTP	Chrome		
2020-04-13 09:53:32	Transfer	213.211.198.58	192.168.1.101	No Authentication Requ...	eicar.com	Malware	Malware Block	HTTP	Chrome		
2020-04-13 09:53:32	Transfer	213.211.198.58	192.168.1.101	No Authentication Requ...	eicar.com	Malware	Malware Block	HTT	Chrome		
2020-04-13 09:53:32	Transfer	213.211.198.58	192.168.1.101	No Authentication Requ...	eicar.com	Malware	Malware Block	HTTP	Chrome		
2020-04-13 09:53:38	Transfer	213.211.198.58	192.168.1.101	No Authentication Requ...	eicar.com	Malware	Malware Block	HTTP	Chrome		

- 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

```
cmd 選択コマンドプロンプト
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>ping 8.8.8.8 ①
8.8.8.8 に ping を送信しています 32 バイトのデータ:
8.8.8.8 からの応答: バイト数 =32 時間 =3ms TTL=50
8.8.8.8 の ping 統計:
    パケット数: 送信 = 4、受信 = 4、損失 = 0 (0% の損失)、
ラウンド トリップの概算時間 (ミリ秒):
    最小 = 3ms、最大 = 3ms、平均 = 3ms ②
C:\Users\Administrator>.
```

- 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

The screenshot shows the Cisco IPS Analysis interface. The 'Analysis' tab is selected, indicated by a blue arrow and a circled '1'. The 'Intrusions > Events' menu item is highlighted, indicated by a blue arrow and a circled '2'. Below the navigation, a message is listed: 'Message' with a sub-entry 'PROTOCOL-ICMP PING (1:384:8)', indicated by a blue arrow and a circled '3'.

- 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

The screenshot shows the 'Events By Priority and Classification' table. The table has columns for Time, Priority, Impact, Inline Result, Source IP, Source Country, Destination IP, Destination Country, Source Port / ICMP Type, Destination Port / ICMP Code, SSL Status, VLAN ID, Message, Classification, and Generator. A single event is listed:

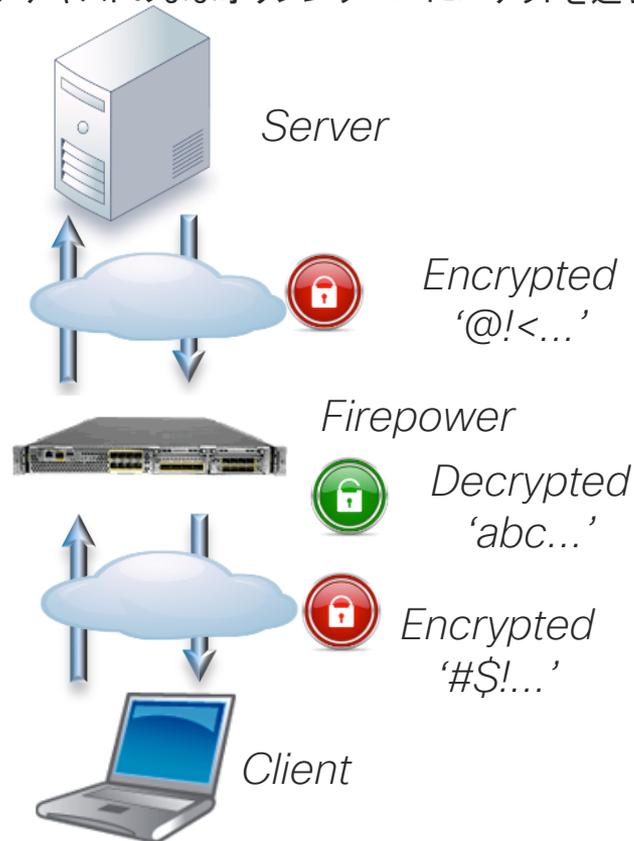
Time	Priority	Impact	Inline Result	Source IP	Source Country	Destination IP	Destination Country	Source Port / ICMP Type	Destination Port / ICMP Code	SSL Status	VLAN ID	Message	Classification	Generator
2020-04-13 09:48:47	low	2	↓	192.168.1.101	8.8.8.8	USA	8.(Echo Request) / icmp	0.(No Code) / icmp	Unknownn.(Unknown)	0	PROTOCOL-ICMP PING (1:384:8)	Misc Activity	Standard Text Rule	

10. TLS Decryptionの設定

TLS 暗号化アクセラレーション

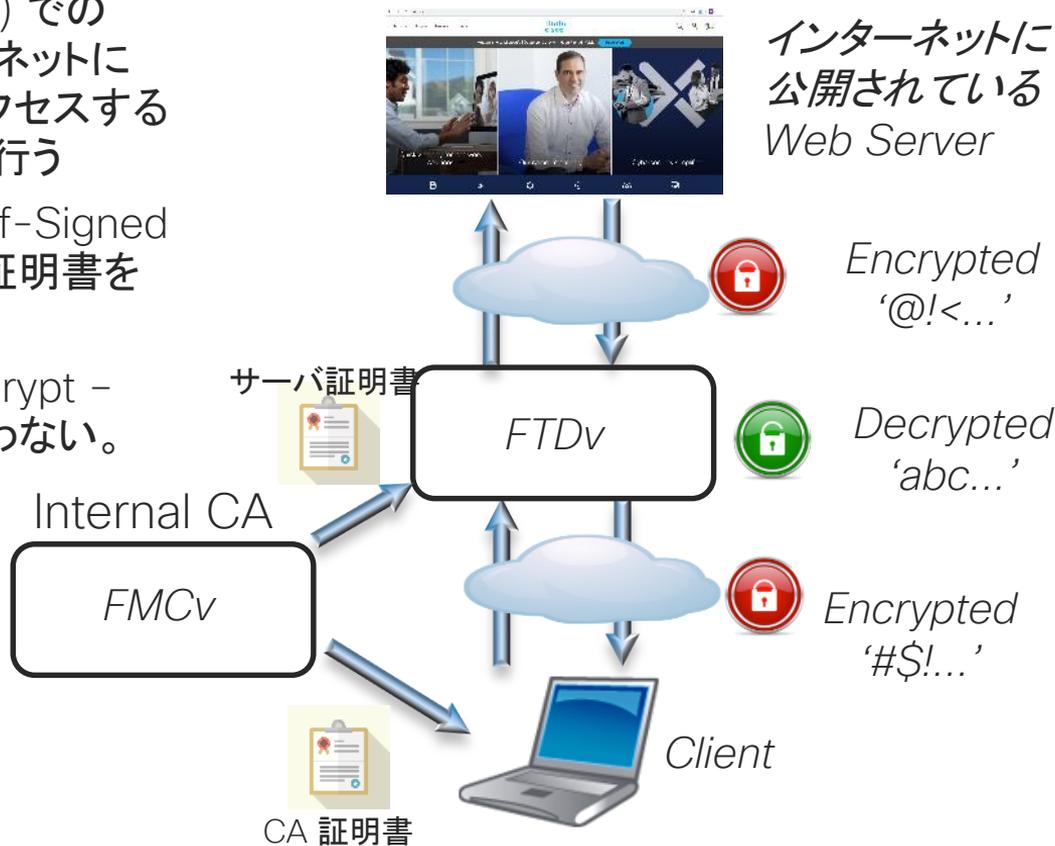
- SSL/TLS で暗号化された通信を復号してインスペクションを行う機能
 - inbound inline (L1), transparent (L2), routed (L3)
 - Decrypt - Known Key 設定を利用
 - 主に不特定多数の端末から自身が管理している公開サーバへの通信を復号 (主に IPS として利用される場合が多い)
 - outbound inline (L1), transparent (L2), routed (L3)
 - Decrypt - Resign 設定を利用
 - 主に自身が管理しているネットワーク内から不特定多数の公開サーバへの通信を復号 (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

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)



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。



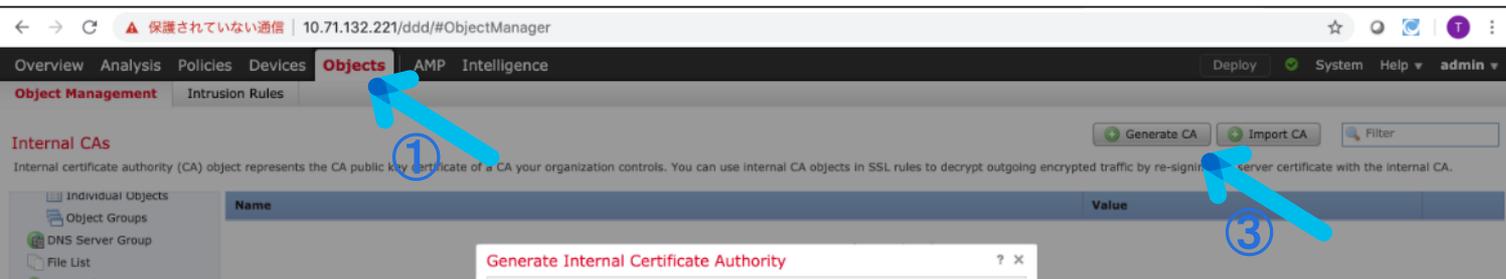
インターネットに
公開されている
Web Server

Encrypted
'@!<...'

Decrypted
'abc...'

Encrypted
'#\$!...'

ステップ1-1: FMC での Internal CA 作成



Generate Internal Certificate Authority

Name:

Country Name (two-letter code):

State or Province:

Locality or City:

Organization:

Organizational Unit (Department):

Common Name:

- 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。そのためまずは Internal CA の PKCS #12 形式のファイルを手にする

Edit Internal Certificate Authority

Name: FMC-CA

Subject:

- Common Name: FMC
- Organization: CiscoSystemsGK
- Organization Unit: GSSO-JP

Issuer:

- Common Name: FMC
- Organization: CiscoSystemsGK
- Organization Unit: GSSO-JP

Not Valid Before:

- Apr 3 05:15:19 2020 GMT

Not Valid After:

- Apr 1 05:15:19 2030 GMT

Serial Number:

- 84:dd:2a:1a:6f:58:bb:57

Certificate Fingerprint:

- D4:B6:BA:EB:4F:AF:35:13:A2:A6:37:FD:49:38:C5:4B:45:3C:C2:50

Public Key Fingerprint:

- 63f1968b44fc34288...9a5f...27c5c6

Download

Encrypt Download File

Password:

Confirm Password:

Passwords Match: ✓

OK Cancel

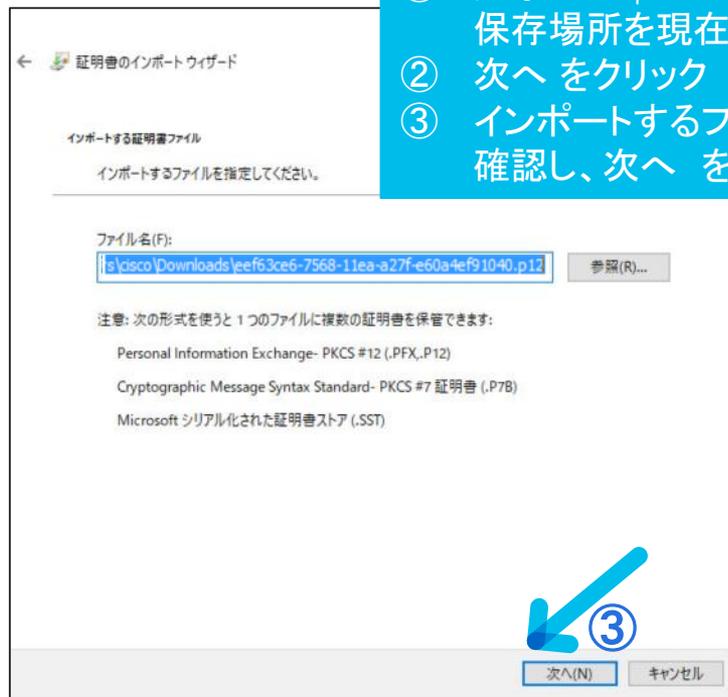
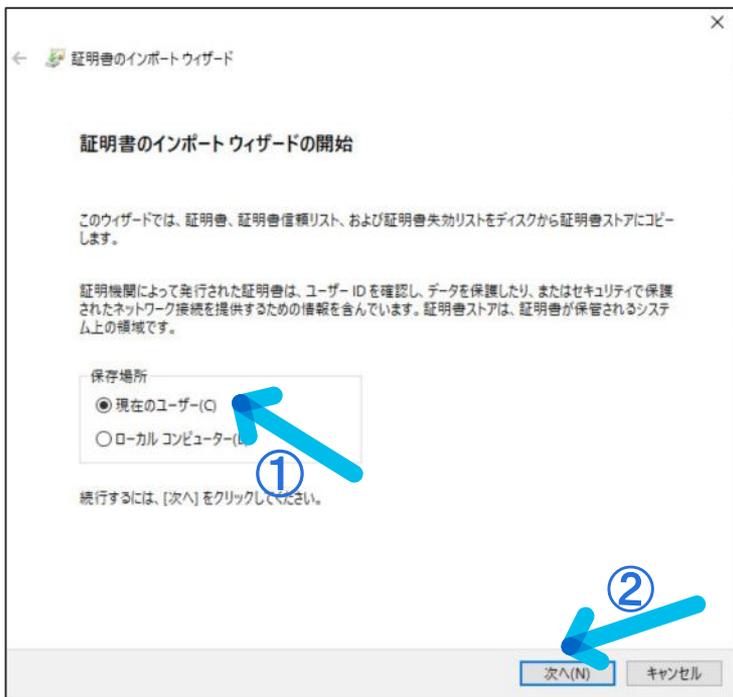
Public eef63ce6-756...p12

- 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

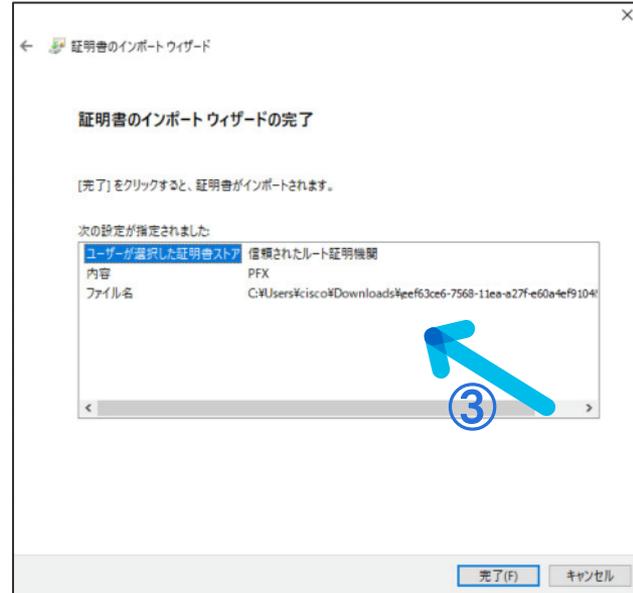
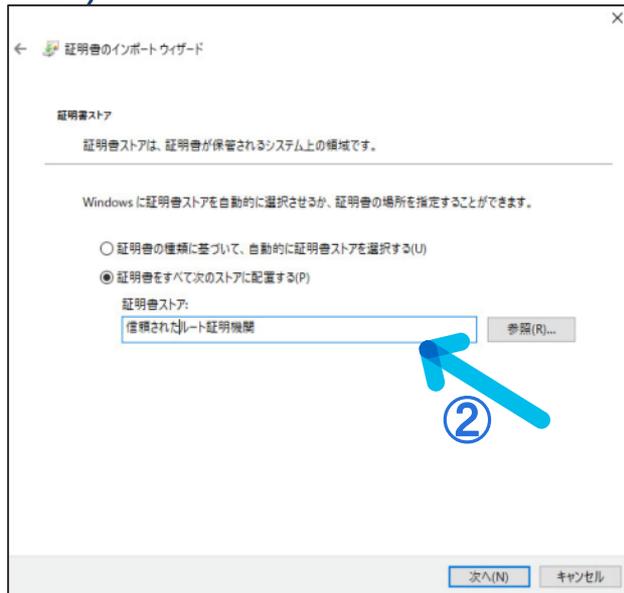
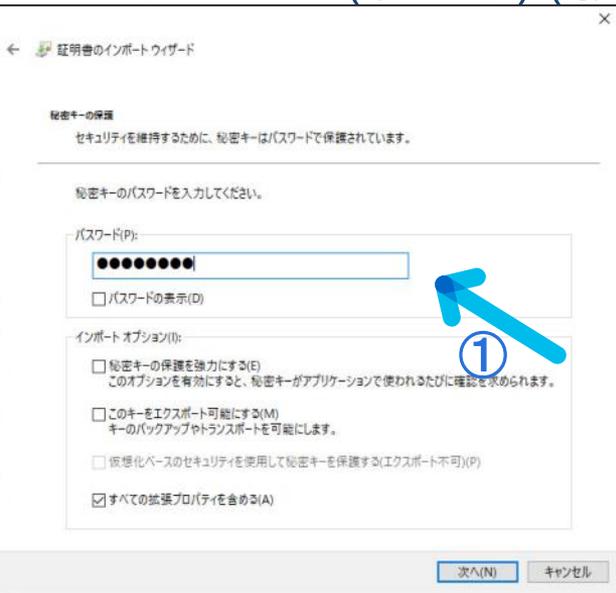
ステップ2-2: PC への Internal CA 証明書のインポート(参考)(続き)

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

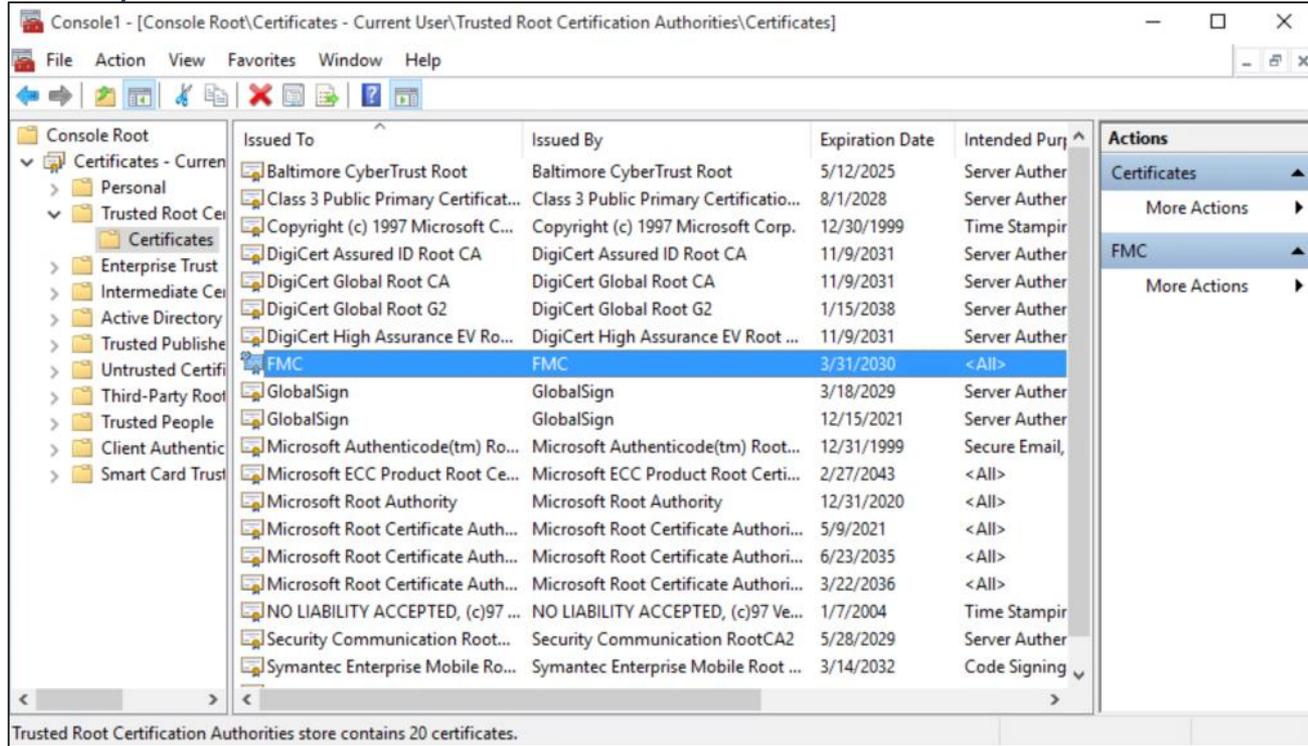
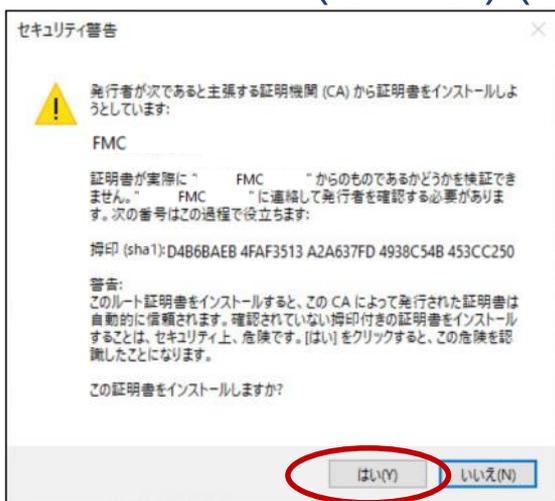


ステップ2-3: PC への Internal CA 証明書のインポート(参考)(続き)



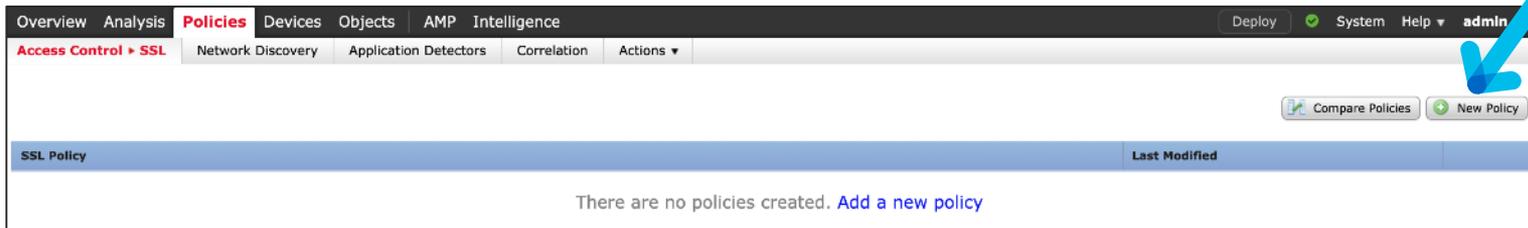
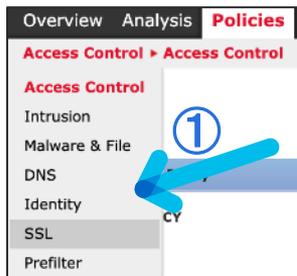
- ① FMC で設定した PKCS #12 のパスワードを入力し、次へ をクリック
- ② マニュアルで証明書ストアに「信頼されたルート証明機関」を選択し、次へ をクリック
- ③ ファイル名や証明書ストアが正しいことを確認し、次へ をクリック

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



New SSL Policy

Name:

Description:

Default Action: Do not decrypt Block Block with reset

Save Cancel

③

④

⑤

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、条件によっては復号の有無を制定した方が良いでしょう。

- 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

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy System H

Access Control > SSL Network Discovery Application Detectors Correlation Actions

SSL-POLICY

Enter Description

Rules Trusted CA Certificates Undecriptable Actions

Name Source

Add Rule

Name DECRYPT-ALL Enabled

Action Decrypt - Resign with FMC-CA Replace Key Only

Insert into Category Standard Rules

Zones Networks VLAN Tags Users Applications Ports Category Certificate DN Cert Status Cipher Suite Version Logging

Available Zones Source Zones (0) Destination Zones (0)

Search by name

inside_zone

outside_zone

Add Rule

Name DECRYPT-ALL Enabled Insert into Category Standard Rules

Action Decrypt - Resign with FMC-CA Replace Key Only

Zones Networks VLAN Tags **Users** Applications Ports Category Certificate DN Cert Status Cipher Suite Version Logging

Log at End of Connection

Send Connection Events to:

Event Viewer

Syslog Server (Using default syslog configuration in Access Control Logging) Show Overrides

SNMP Trap Select an SNMP Alert Configuration...

Add Cancel

ステップ3-3: SSL policy のルール作成 (続き)

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

Access Control > SSL Network Discovery Application Detectors Correlation Actions

SSL-POLICY You have unsaved changes Save Cancel

Enter Description

Rules Trusted CA Certificates Undecryptable Actions

+ Add Category + Add Rule Search Rules

#.	Name	Source Zo...	Dest Zones	Source Netw...	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	Categories	SSL	Action
Administrator Rules													
This category is empty													
Standard Rules													
1	DECRYPT-ALL	any	any	any	any	any	any	any	any	any	any	any	Decrypt - Resign
Root Rules													
This category is empty													
Default Action													
												Do not decrypt	

- 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

Access Control Policy	Status	Last Modified
ACCESS-POLICY	Targeting 1 devices Up-to-date on all targeted devices	2020-03-27 10:09:18 Modified by "admin"

SSL Policy: SSL-POLICY

Identity Policy: None

SSL Policy to use for inspecting encrypted connections

SSL-POLICY

Revert to Defaults OK Cancel

ステップ5-1: 設定の反映

The screenshot shows the Cisco FMC interface with the 'Deploy Policies' dialog box open. The dialog title is 'Deploy Policies' with a version timestamp of '2020-04-03 07:24 PM'. A yellow warning banner at the top of the dialog states: 'All Firepower Threat Defense devices may have Inspect Interruption. For details, see [online help](#)'. Below this is a table with columns: Device, Inspect Interruption, Type, Group, and Current Version. The table contains one entry for device 'FTDv01' with 'Inspect Interruption' set to 'Yes', 'Type' as 'FTD', and 'Current Version' as '2020-04-03 01:29 PM'. A list of policies is shown below the table, each with a status icon (green checkmark for active, grey circle for inactive): FlexConfig Policy (active), Access Control Policy: ACCESS-POLICY (inactive), Intrusion Policy: Balanced Security and Connectivity (active), Intrusion Policy: No Rules Active (active), File Policy: FILE-POLICY (active), Intrusion Policy: INTRUSION-POLICY (active), DNS Policy: Default DNS Policy (active), SSL Policy: SSL-POLICY (inactive), Prefilter Policy: Default Prefilter Policy (active), Network Discovery (active), Device Configuration(Details) (active), and Rule Update (2020-02-19-001-vrt) (active). The main interface in the background shows the 'Policies' tab and the 'Deploy' button in the top right corner.

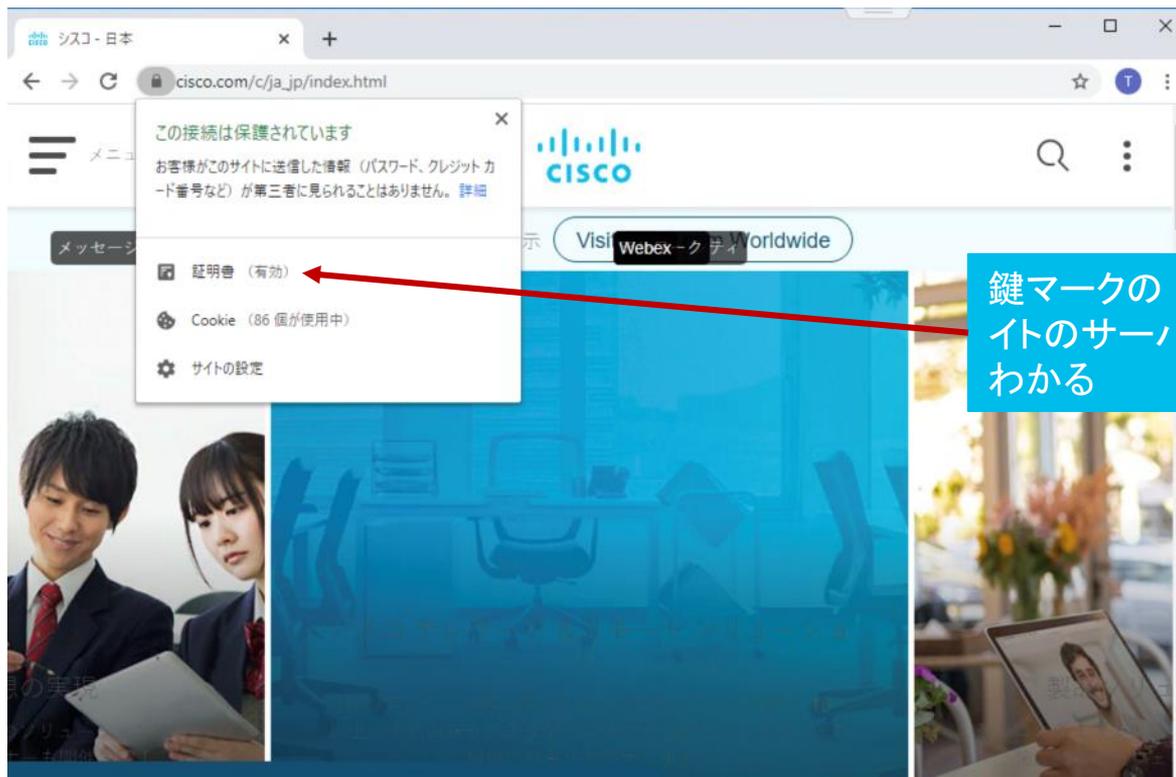
FMC 画面右上部の Deploy をクリックし、該当の FTD を選択 + をクリックするところ変更される箇所がわかる

本シナリオでは ACP と SSL Policy が変更され、SSL Policy の適用により Short 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を確認できる



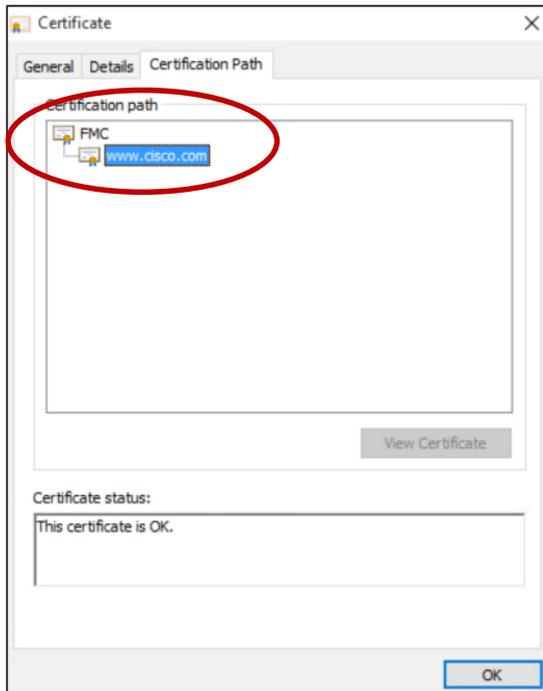
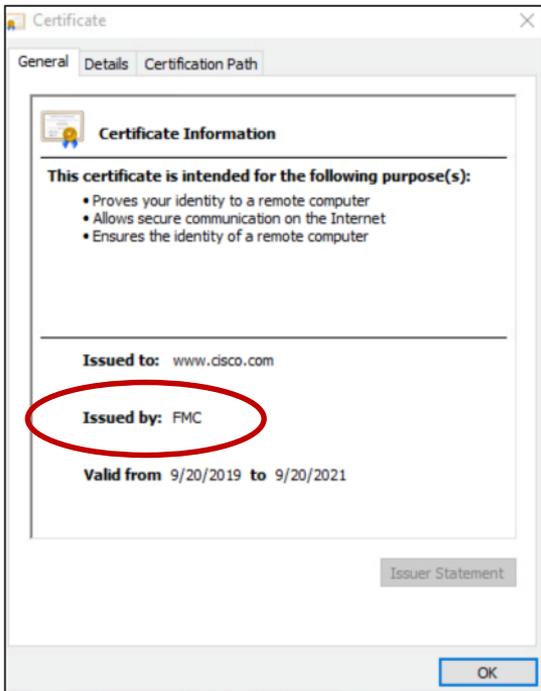
鍵マークの“証明書 (有効)”をクリックすると、このサイトのサーバ証明書をどこの CA がサインしたかがわかる

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

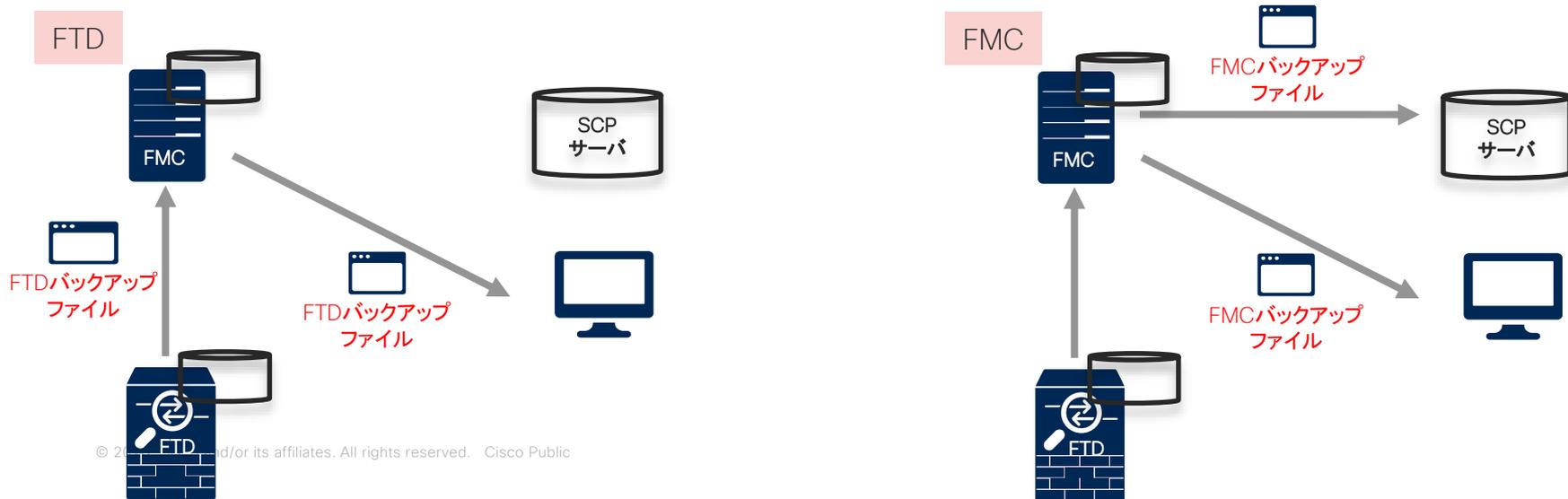
The screenshot shows the Cisco FMC interface with the 'Connection Events' table in 'Table View'. The table is filtered for outgoing HTTPS traffic. A red box highlights the 'SSL Status' column, which shows 'Decrypt (Resign)' for several entries, indicating that the outgoing traffic is being decrypted.

Source Port / ICMP Type	Destination Port / ICMP Code	SSL Status	Application Protocol	Client	Client Version	Web Application	Application Risk	Business Relevance	URL	URL Category
61402 / tcp	443 (https) / tcp		HTTPS	SSL client		Cisco	Medium	Medium	https://cisco-tags.cisco.com	Business and Eco
61401 / tcp	443 (https) / tcp		HTTPS	SSL client			Medium	Medium	https://gallery.sprinkr.com	Computer and Int
61400 / tcp	443 (https) / tcp		HTTPS	SSL client			Medium	Medium	https://col.eum-apodynamics.com	Computer and Int
61399 / tcp	443 (https) / tcp	Decrypt (Resign)	HTTP	Chrome	80.0.3987.163	Cisco	Medium	Medium	https://conductor.clicktale.net/monitor?t=chunk&p=...	Computer and Int
55667 / udp	53 (domain) / udp		DNS	DNS client			Very Low	Very High		
61399 / tcp	443 (https) / tcp		HTTPS	SSL client		ClickTale	Medium	Very Low	https://conductor.clicktale.net	Computer and Int
61398 / tcp	443 (https) / tcp	Decrypt (Resign)	HTTP	Chrome	80.0.3987.163	Cisco	Medium	Medium	https://col.eum-apodynamics.com/eumcollector/beaco...	Computer and Int
61398 / tcp	443 (https) / tcp		HTTPS	SSL client			Medium	Medium	https://col.eum-apodynamics.com	Computer and Int
61397 / tcp	443 (https) / tcp	Decrypt (Resign)	HTTP	Chrome	80.0.3987.163	Cisco	Medium	Medium	https://cisco-tags.cisco.com/tag/toanotag.gif?js=...	Business and Eco
61397 / tcp	443 (https) / tcp		HTTPS	SSL client		Cisco	Medium	Medium	https://cisco-tags.cisco.com	Business and Eco
61396 / tcp	443 (https) / tcp	Decrypt (Resign)	HTTP	Chrome	80.0.3987.163	Cisco	Medium	Medium	https://gallery.sprinkr.com/clients/1035/embeds/Z...	Computer and Int
61396 / tcp	443 (https) / tcp		HTTPS	SSL client			Medium	Medium	https://gallery.sprinkr.com	Computer and Int
53830 / udp	53 (domain) / udp		DNS	DNS client			Very Low	Very High		
61395 / tcp	443 (https) / tcp	Decrypt (Resign)	HTTP	Chrome	80.0.3987.163	Cisco	Medium	Medium	https://ing-district.clicktale.net/ctn_v2/wr/72717...	Computer and Int
61394 / tcp	443 (https) / tcp									
52318 / udp	53 (domain) / udp		DNS	DNS client			Very Low	Very High		
61394 / tcp	443 (https) / tcp		HTTPS	SSL client		Microsoft	Medium	Low	https://settings-win.data.microsoft.com	Business and Eco
55245 / udp	53 (domain) / udp		DNS	DNS client			Very Low	Very High		

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

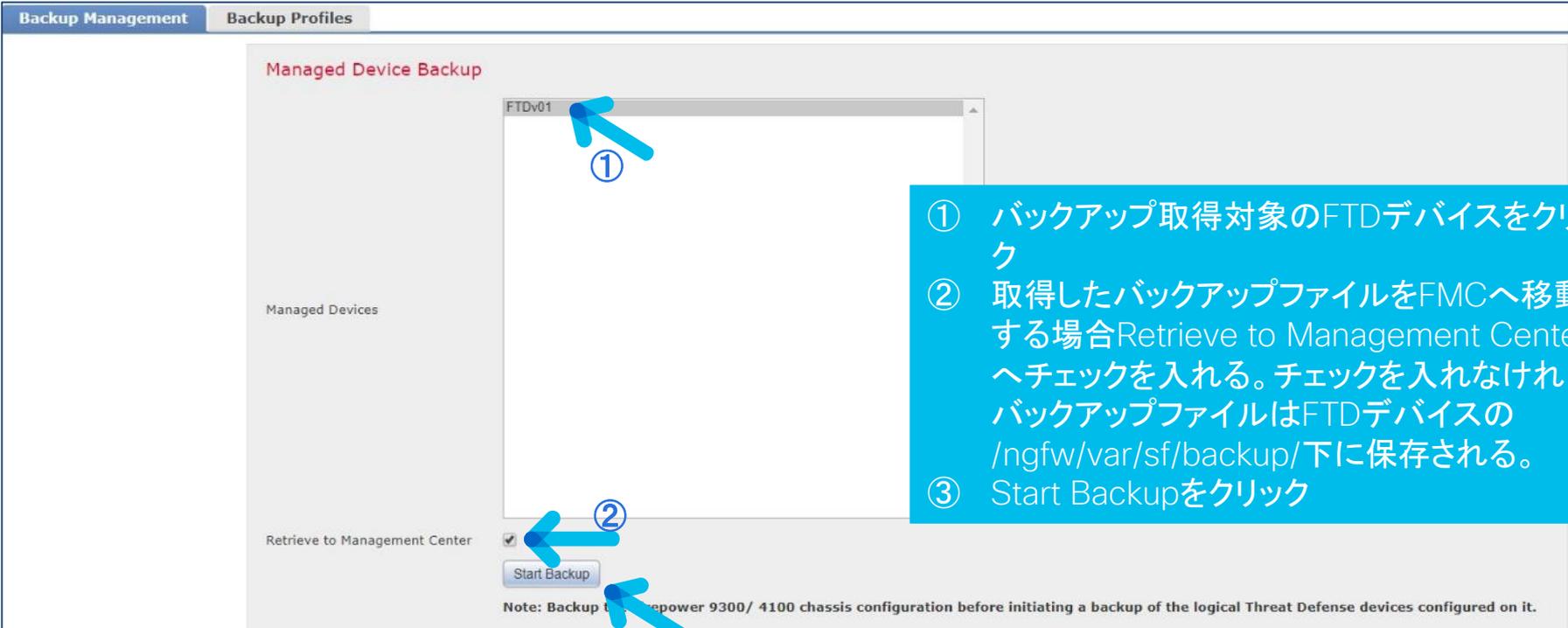
- ・ FMCの管理下にあるFTDデバイスのバックアップを取得する。



- 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。



Backup Management Backup Profiles

Managed Device Backup

Managed Devices

FTDv01

Retrieve to Management Center

Start Backup

Note: Backup to Management Center requires power 9300/ 4100 chassis configuration before initiating a backup of the logical Threat Defense devices configured on it.

- 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。

The screenshot shows the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Tasks' tab is selected, showing a summary of task status: '20+ total', '0 waiting', '1 running', and '20+ success'. A task named 'Backup: FTDv01_20200420141640' is highlighted in a red box, with the description 'Backing up the database tables'. Below this, a list of tasks is shown, including 'Local Install', 'Download from Sourcefire support site', 'Backup (Scheduled)', and 'Policy Deployment'. Blue arrows and numbered circles (1, 2, 3) indicate the steps to navigate to this task: 1. Click the 'System' icon in the top right. 2. Click the 'Tasks' tab. 3. Click the task name 'Backup: FTDv01_20200420141640'.

- ① Systemの隣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。



Overview Analysis Policies Devices Objects AMP Intelligence System Help admin

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools Backup/Restore Remote Storage

Backup Management Backup Profiles Firepower Management Backup Managed Device Backup Upload Backup

①



Device Backups

System Information	Date Created	File Name	VDB Version	Location	Size (MB)	Configurations	Events
FTDv01 Cisco Firepower Threat Defense for VMWare v6.4.0.7	2020-04-20 14:20:10	FTDv01_20200420141640.tar	build 332	Local	70	Yes	No

Download Delete Move

②

- 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。

Backup Management Backup Profiles

Create Backup

Name	FMC BACKUP 20200420
Storage Location	/var/sf/backup/
Back Up Configuration	<input checked="" type="checkbox"/>
Back Up Events	<input type="checkbox"/>
Email	Not available. You must set up your mail relay host.
Copy when complete	<input type="checkbox"/>

Start Backup Save As New Cancel

- 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。

Backup Management Backup Profiles

Create Backup

Name	<input type="text" value="FMC BACKUP 20200420"/>
Storage Location	<input type="text" value="/var/sf/backup/"/>
Back Up Configuration	<input checked="" type="checkbox"/>
Back Up Events	<input type="checkbox"/>
Email	<u>Not available. You must set up your mail relay host.</u>
Copy when complete	<input checked="" type="checkbox"/>
Host	<input type="text" value="10.70.78.1"/> ①
Path	<input type="text" value="/home/"/> ②
User	<input type="text" value="admin"/> ③
Password	<input type="password" value="....."/> ④
SSH Public Key	<input type="text" value="ssh-rsa AAAAB3NzaC1yc2EAAAADAQ..."/> ④

To use ssh keys place this public key in your authorized_keys file.

- 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。

The screenshot shows the Cisco FMC backup management interface. The 'Backup Management' section is active, displaying a 'Create Backup' form with fields for Name, Storage Location, Back Up Configuration, Back Up Events, Email, Copy when complete, and Host. The 'Task Notification' section shows a list of tasks, including 'Backup: FMC BACKUP 20200420' which is highlighted with a red box and a blue arrow labeled '3'. The 'Tasks' tab is selected, and the 'System' icon is highlighted with a blue arrow labeled '1'. The 'Tasks' tab shows a summary of 20+ total tasks, with 2 running and 20+ success.

- 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。

The screenshot shows the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. On the right, there are buttons for 'Deploy', 'System', 'Help', and 'admin'. Below the navigation bar, there are tabs for 'Configuration', 'Users', 'Domains', 'Integration', 'Updates', 'Licenses', 'Health', and 'Monitoring'. A 'Tools' menu is open, showing 'Backup/Restore' and 'Remote Storage'. The 'Backup Management' tab is selected, and a blue arrow points to it with a circled '1'. Below this, there are buttons for 'Firepower Management Backup', 'Managed Device Backup', and 'Upload Backup'. The 'Firepower Management Backups' section contains a table with the following data:

System Information	Date Created	File Name	VDB Version	Location	Size (MB)	Configurations	Events
EMCV Cisco Firepower Management Center for VMWare v6.4.0.7	2020-04-20 14:27:41	FMC_BACKUP_20200420-2020-04-20T05-19-49.tar	build 332	Local	221	Yes	No

A red box highlights the table, and a blue arrow points to the file name with a circled '2'.

- 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。

New Task

Job Type ①

Schedule task to run Once Recurring ②

Start On Asia/Tokyo ③

Repeat Every ④ Hours Days Weeks Months

Run At

Repeat On Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Job Name ⑤

Backup Type Management Centre Device ⑥

Backup Profile ⑦

Comment

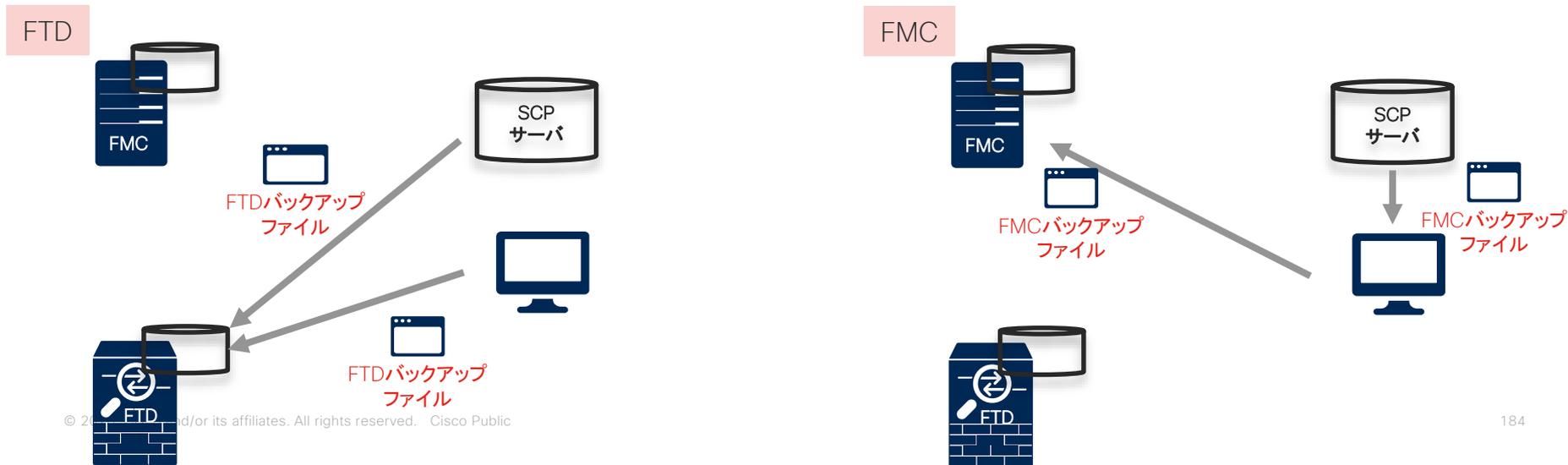
Email Status To Not available. You must set up your mail relay host.

⑧

- 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。

The screenshot shows the Cisco FMC Backup/Restore interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The right side of the navigation bar shows 'Deploy', 'System', 'Help', and 'admin'. Below the navigation bar, there are tabs for 'Configuration', 'Users', 'Domains', 'Integration', 'Updates', 'Licenses', 'Health', and 'Monitoring'. The 'Tools' menu is open, showing 'Backup/Restore' and 'Remote Storage'. The 'Backup Management' section is active, and the 'Backup Profiles' tab is selected. The main content area displays the 'Upload Backup' section with the text 'Please Select a File to Upload'. There are two buttons: 'ファイルを選択' (Select File) and 'Upload Backup'. A red arrow points to the 'ファイルを選択' button, labeled with a circled '1'. A blue arrow points to the 'Upload Backup' button, labeled with a circled '2'.

- 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。



The screenshot displays the Cisco FMC web interface. At the top, there is a navigation bar with tabs for Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. On the right side of the navigation bar, there are buttons for Deploy, System, Help, and admin. Below the navigation bar, there is a secondary menu with tabs for Configuration, Users, Domains, Integration, Updates, Licenses, Health, and Monitoring. On the far right of this menu, there is a link for Tools > Backup/Restore. Below the secondary menu, there is a button for Remote Storage. The main content area shows a 'Backup Management' section with a 'Backup Profiles' tab. A green success message box is displayed, stating: 'Success Backup 'FMC_BACKUP_20200420-2020-04-20T05-19-49.tar' uploaded successfully'. A blue arrow points to the success message box, and a red circle with the number 1 is placed next to it. Below the success message, there is an 'Upload Backup' section with the text 'Please Select a File to Upload'. There is a button labeled 'ファイルを選択' (Select File) and a message '選択されていません' (Not selected). Below this, there is an 'Upload Backup' button.

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。

The screenshot shows the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'System' tab is active, and the 'Backup/Restore' section is selected. The 'Backup Profiles' tab is highlighted with a blue arrow and a circled '1'. Below this, the 'Firepower Management Backups' section is visible, containing a table with the following data:

System Information	Date Created	File Name	VDB Version	Location	Size (MB)	Configurations	Events
FMCV Cisco Firepower Management Center for VMWare v6.4.0.7	2020-04-24 17:40:39	<u>FMC_BACKUP_20200420-2020-04-20T05-19-49.tar</u>	build 332	Local	221	Yes	No

A red box highlights the backup file row, and a blue arrow points to the file name with a circled '2'.

- 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。

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Configuration Users Domains Integration Updates Licenses Health Monitoring **Tools ▶ Backup/Restore**

Backup Management Backup Profiles Firepower Management Backup Managed Device Backup Upload Backup

Firepower Management Backups

System Information	Date Created	File Name	VDB Version	Location	Size (MB)	Configurations	Events
<input checked="" type="checkbox"/> FMCv Cisco Firepower Management Center for VMWare v6.4.0.7	2020-04-20 14:27:41	FMC_BACKUP_20200420-2020-04-20T05-19-49.tar	build 332	Local	221	Yes	No
<input type="checkbox"/> FMCv Cisco Firepower Management Center for VMWare v6.4.0.7	2020-04-19 11:08:03	Weekly_config_only_backup_20200419020002-2020-04-19T02-00-04.tar	build 332	Local	221	Yes	No
<input type="checkbox"/> FMCv Cisco Firepower Management Center for VMWare v6.4.0.7	2020-04-12 11:06:45	Weekly_config_only_backup_20200412020002-2020-04-12T02-00-04.tar	build 332	Local	219	Yes	No
<input type="checkbox"/> FMCv Cisco Firepower Management Center for VMWare v6.4.0.7	2020-04-05 11:07:46	Weekly_config_only_backup_20200405020002-2020-04-05T02-00-03.tar	build 332	Local	218	Yes	No
<input type="checkbox"/> FMCv Cisco Firepower Management Center for VMWare v6.4.0.7	2020-03-29 11:06:06	Weekly_config_only_backup_20200329020002-2020-03-29T02-00-04.tar	build 332	Local	215	Yes	No
<input type="checkbox"/> FMCv Cisco Firepower Management Center for VMWare v6.4.0.7	2020-03-22 11:07:16	Weekly_config_only_backup_20200322020002-2020-03-22T02-00-03.tar	build 332	Local	216	Yes	No
<input type="checkbox"/> FMCv Cisco Firepower Management Center for VMWare v6.4.0.7	2020-03-15 11:09:53	Weekly_config_only_backup_20200315020002-2020-03-15T02-00-04.tar	build 332	Local	218	Yes	No
<input type="checkbox"/> FMCv Cisco Firepower Management Center for VMWare v6.4.0.7	2020-03-08 11:06:16	Weekly_config_only_backup_20200308020002-2020-03-08T02-00-04.tar	build 309	Local	214	Yes	No
<input type="checkbox"/> FMCv Cisco Firepower Management Center for VMWare v6.4.0.7	2020-03-01 11:05:27	Weekly_config_only_backup_20200301020002-2020-03-01T02-00-04.tar	build 332	Local	218	Yes	No
<input type="checkbox"/> FMCv Cisco Firepower Management Center for VMWare v6.4.0.7	2020-02-23 11:05:31	Weekly_config_only_backup_20200223020002-2020-02-23T02-00-04.tar	build 332	Local	218	Yes	No

Restore Download Delete Move

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。

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy System Help admin

Remote Storage

Info
You are about to replace or modify key system files.
The system will be rebooted at the end of the restore process.

Restore Backup

Backup Name FMC_BACKUP_20200420-2020-04-20T05-19-49.tar

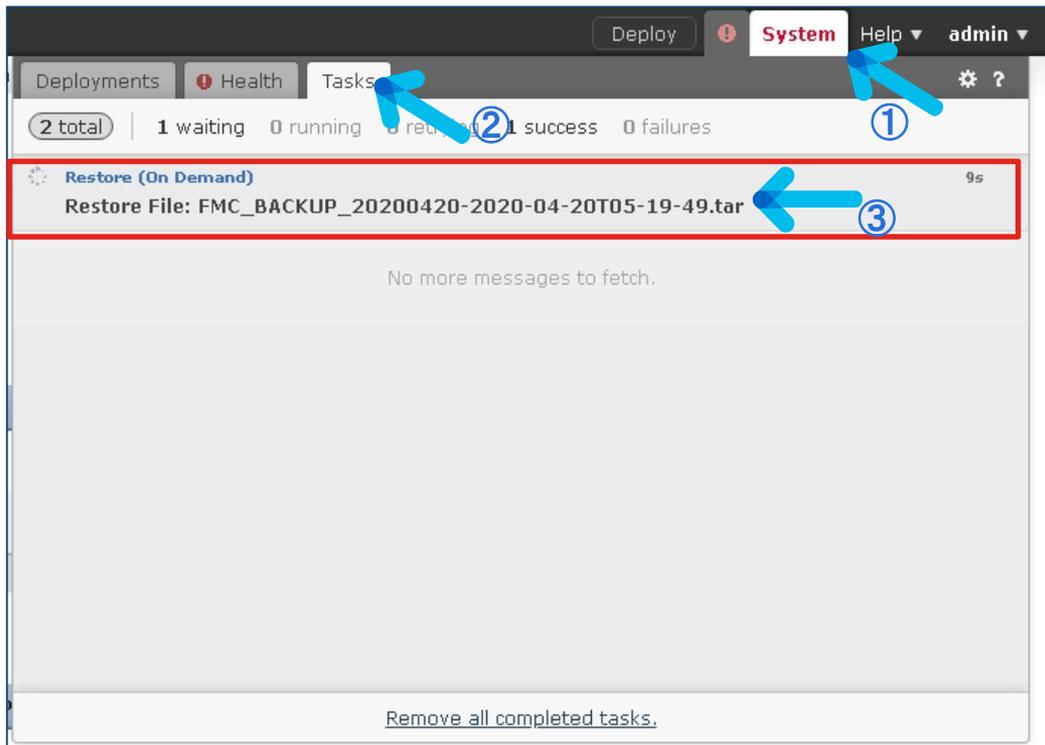
Replace Configuration Data ①

Restore ② Cancel

- 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。

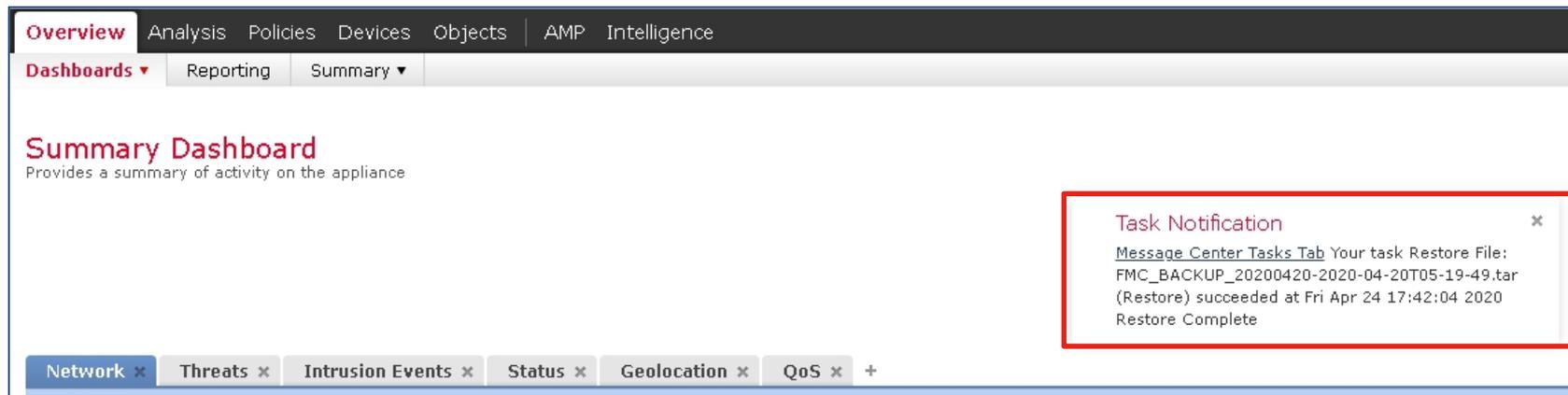


- ① Systemの隣のアイコンをクリック
- ② Tasksを選択
- ③ “Restore”という項目名の下で”Restore File”の名前でタスクが進行しているを確認できる。

- ・ 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。



The screenshot displays the Cisco FMC web interface. At the top, there is a navigation bar with tabs for Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. Below this is a sub-navigation bar with 'Dashboards' selected, showing 'Reporting' and 'Summary' options. The main content area is titled 'Summary Dashboard' and includes the text 'Provides a summary of activity on the appliance'. On the right side, a 'Task Notification' box is highlighted with a red border. The notification text reads: 'Message_Center_Tasks_Tab Your task Restore File: FMC_BACKUP_20200420-2020-04-20T05-19-49.tar (Restore) succeeded at Fri Apr 24 17:42:04 2020 Restore Complete'. At the bottom of the dashboard, there is a row of tabs for 'Network', 'Threats', 'Intrusion Events', 'Status', 'Geolocation', and 'QoS', each with a close icon (x) and a plus sign (+) to the right.

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。

```
> restore remote-manager-backup FTDv01_20200424194454.tar
```

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

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 . . . . .
```

```
Are you sure you want to continue (Y/N)Y ← ①
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 . . . . .
```

```
Are you sure you want to continue (Y/N)Y ← ①
Restoring device . . . . .
```

① “Y”を入力

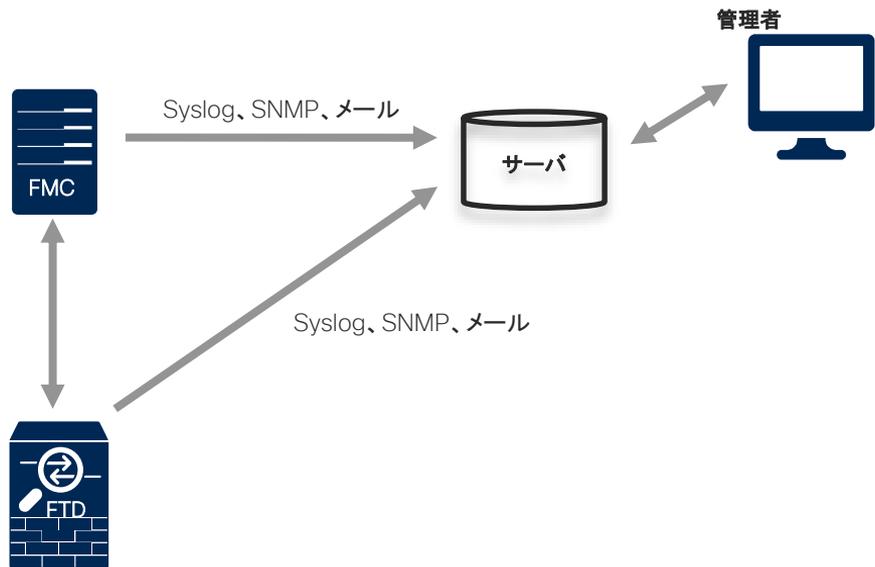
- リストア完了後に機器が再起動

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、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

The screenshot shows the Cisco FTD configuration interface. The top navigation bar includes Overview, Analysis, Policies, **Devices**, Objects, AMP, and Intelligence. Under the **Devices** tab, the **Platform Settings** sub-tab is selected. A table lists the configuration for the **FTD-POLICY**, showing it is for **Threat Defense** and is **Targeting 1 devices**. A blue arrow labeled ① points to the **Platform Settings** tab, and another blue arrow labeled ② points to the edit (pencil) icon in the table's action column.

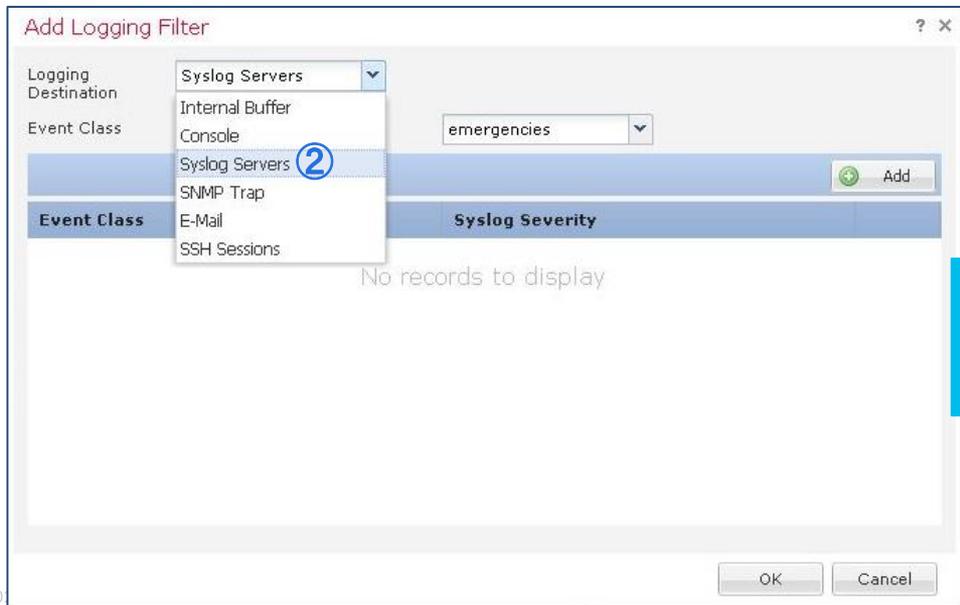
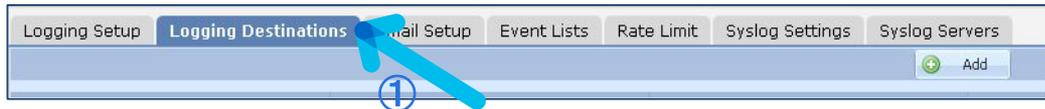
The left sidebar menu shows various configuration options, with **Syslog** highlighted by a blue arrow labeled ③. The main configuration area is titled **Logging Setup** and includes sections for **Basic Logging Settings**, **VPN Logging Settings**, and **Specify FTP Server Information**. In the **Basic Logging Settings** section, the **Enable Logging** checkbox is checked, indicated by a blue arrow labeled ④.

- 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

The image shows two sequential screenshots of the 'Add Logging Filter' dialog box. In the first screenshot, the 'Event Class' dropdown menu is open, and 'Filter on Severity' is selected. In the second screenshot, the 'Filter on Severity' dropdown menu is open, and 'notifications' is selected. The 'OK' button is highlighted in the second screenshot.

- 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

Logging Setup | Logging Destinations | Email Setup | Event Lists | Rate Limit | **Syslog Settings** | Syslog Servers

Facility: LOCAL4(20) ②

Enable Timestamp on Syslog Messages: ③

Timestamp Format: Legacy (MMM dd yyyy HH:mm:ss) ④

Enable Syslog Device ID:

NetFlow Equivalent Syslogs:

Syslog ID	Logging Level	Enabled
106015	(default)	✗
106023	(default)	✗
302013	(default)	✗
302014	(default)	✗
302015	(default)	✗
302016	(default)	✗

- 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

Add Syslog Server

IP Address*

Protocol TCP UDP

Port (514 or 1025-61415)

Log Messages in Cisco EMBLEM format(UDP only)

Enable secure syslog.

Reachable By:

Device Management Interface (Applicable on FTD v6.3.0 and above)

Security Zones or Named Interface

Available Zones

- inside_zone
- outside_zone

Add

Selected Zones/Interfaces

Interface Name Add

OK Cancel

Edit Network Object

Name

Description

Network Host Range Network FQDN

Allow Overrides

Save Cancel

- 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

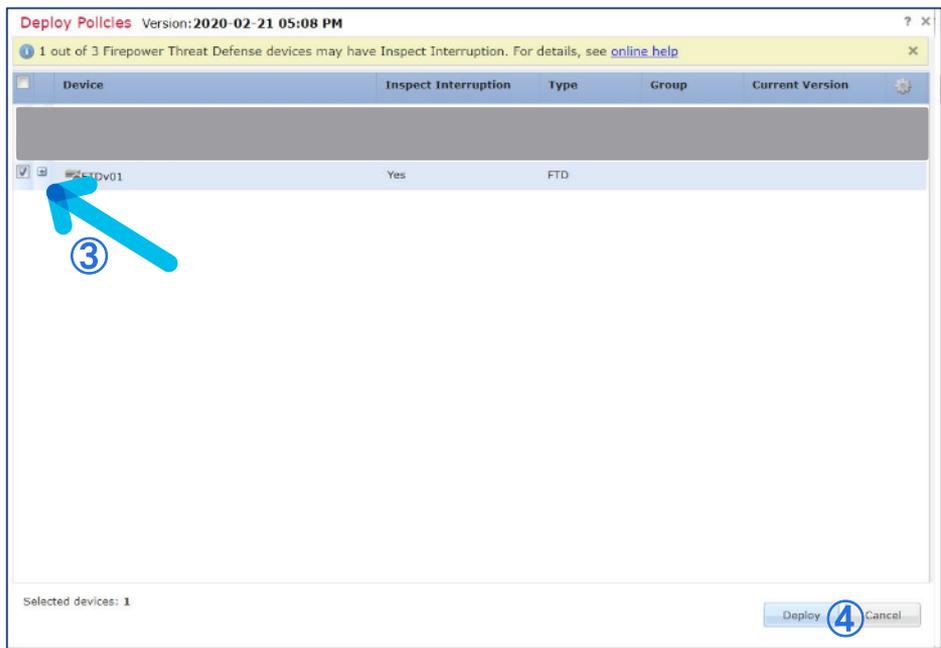
ステップ 4: Syslog Servers設定③

- Syslogメッセージを出力する先のSyslogサーバ設定を行う

① ② ③ ④

- 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GigabitEthernet0/0、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

Policy Name	Domain	Applied To	Last Modified	
Initial_Health_Policy 2020-02-14 04:59:35 Initial Health Policy	Global	3 appliances	2020-02-14 13:59:34 Modified by "admin"	

- 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

Overview Analysis Policies Devices Objects AMP Intelligence

Editing Policy: Initial_Health_Policy 2020-02-14 04:59:35

Policy Name: Initial_Health_Policy 2020-02-14 04:59:35
Policy Description: Initial Health Policy

Policy Run Time Interval

Run Interval (mins): 5

- AMP For Endpoints Status
- AMP for Firepower Status
- Appliance Heartbeat
- Automatic Application Bypass Status
- Backlog Status
- CPU Usage

Overview Analysis Policies Devices Objects AMP Intelligence

Editing Policy: Initial_Health_Policy 2020-02-14 04:59:35

Policy Name: Initial_Health_Policy 2020-02-14 04:59:35
Policy Description: Initial Health Policy

Policy Run Time Interval

AMP For Endpoints Status

Enabled On Off

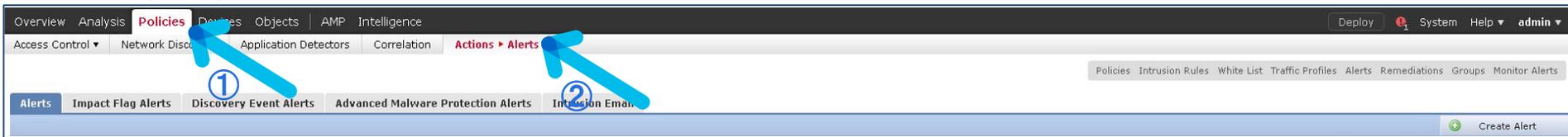
Description: AMP for Endpoints Status

- AMP for Firepower Status
- Appliance Heartbeat
- Automatic Application Bypass Status
- Backlog Status
- CPU Usage

- 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

Edit Syslog Alert Configuration ? x

Name

Host

Port

Facility

Severity

Tag

Alert Configuration is in use by 8 Policies.

- 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。

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy System Help admin

Configuration Users Domains Integration Updates Licenses Health Monitor Alerts Monitoring Tools

Active Health Alerts

Configure Health Alerts

Health Alert Name HEALTH-ALERT

Severity	Module	Alert
Critical	Inline Link Mismatch Alarms	SYSLOG-ALERT (Syslog)
Warning	Interface Status	
Normal	Intrusion and File Event Rate	
Error	Link State Propagation	
Recovered	Local Malware Analysis	
	Memory Usage	
	Platform Faults	
	Power Supply	
	Process Status	
	RRD Server Process	
	Realm	
	Reconfiguring Detection	
	Security Intelligence	
	Smart License Monitor	
	Threat Data Updates on Devices	
	Time Series Data Monitor	
	Time Synchronization Status	
	URL Filtering Monitor	
	User Agent Status Monitor	
	VPN Status	

Threshold Timeout (Optional) (in minutes)

Load Delete Save

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

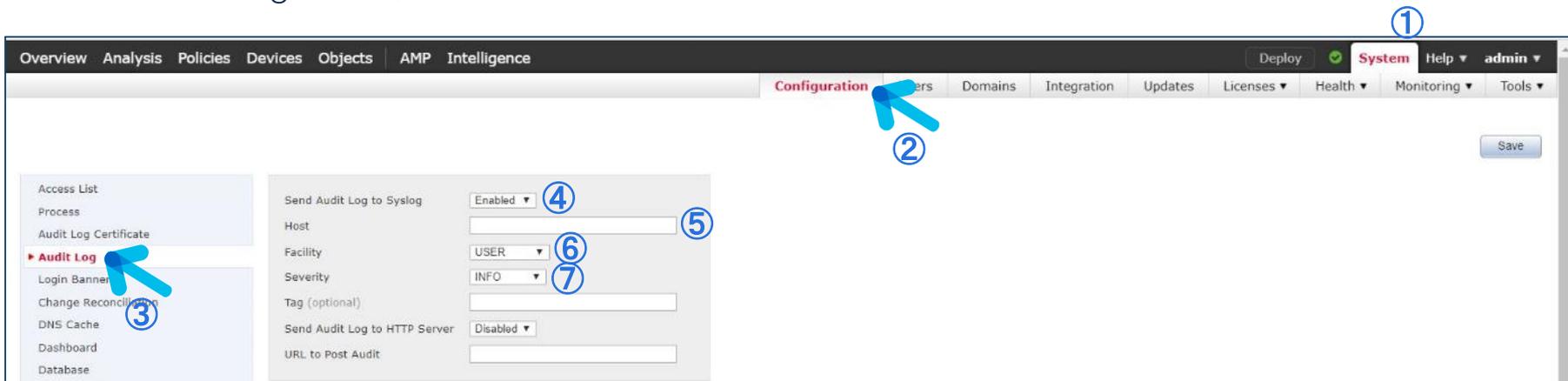
参考: その他のアラート設定について③

- 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

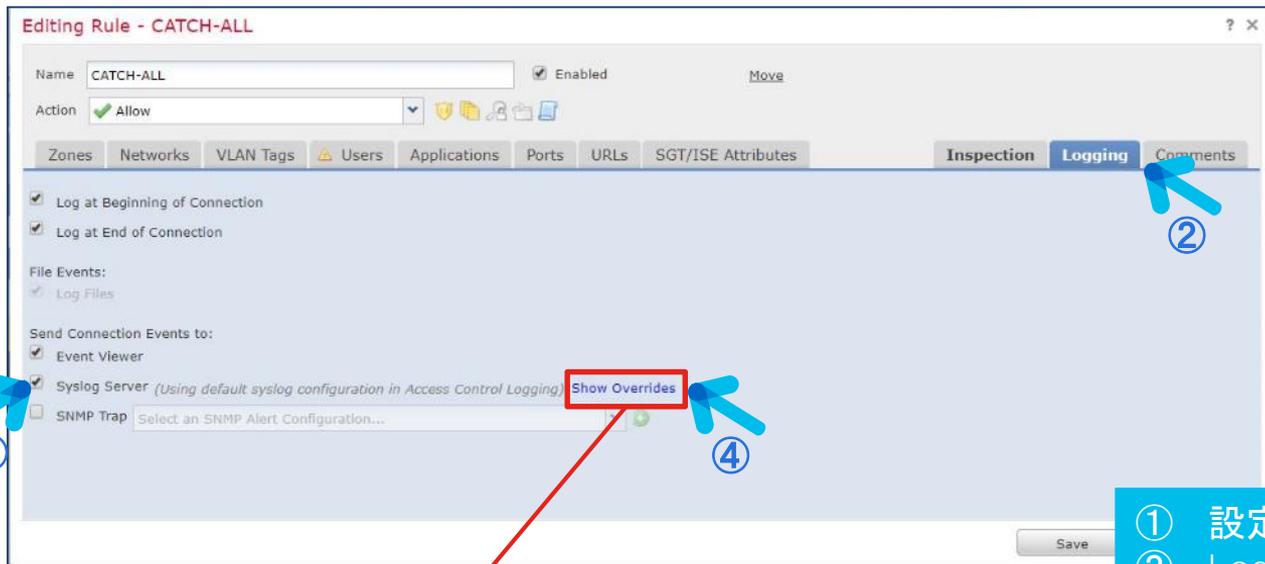
- Connection Event設定画面は次のようになる。

The screenshot displays the 'ACCESS-POLICY' configuration interface. The 'Logging' tab is selected, and the 'Default Syslog Settings' section is visible. The checkbox for 'Send using specific syslog alert' is checked, and the 'Syslog Alert' dropdown is set to 'SYSLOG-ALERT'. A 'Summary' section on the right provides details for different device versions. Blue arrows with circled numbers 1, 2, and 3 highlight the 'Logging' tab, the checkbox, and the dropdown menu, respectively.

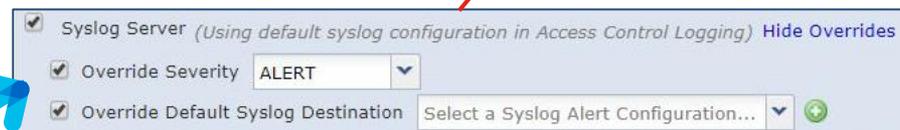
- ① 設定対象とするAccess policyを開く
- ② Loggingを選択[Send using specific syslog alert]にチェックを入れる
- ③ 使用するSyslog Alertをプルダウンより選択

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。



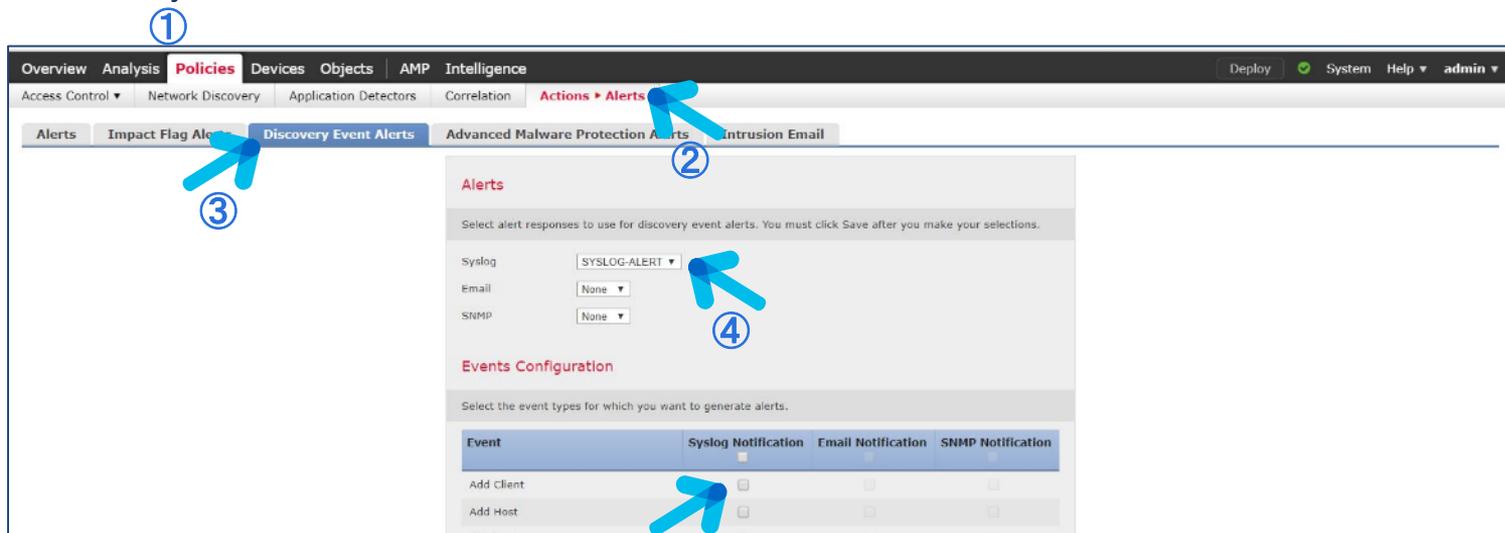
- ① 設定対象とするAccess Ruleを開く
- ② Loggingを選択
- ③ Syslog Serverにチェックを入れる
- ④ Show Overridesをクリック
- ⑤ Overrideさせる設定として、Severity、使用するSyslog Alertを指定



⑤

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

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

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

Alerts **Impact Flag Alerts** Discovery Event Alerts Advanced Malware Protection Alerts Intrusion Email

Alerts

Select alert responses to use for Impact Flag alerts. You must click Save after you make your selections.

Syslog: SYLOG-ALERT

Email: None

SNMP: None

Impact Flag Configuration

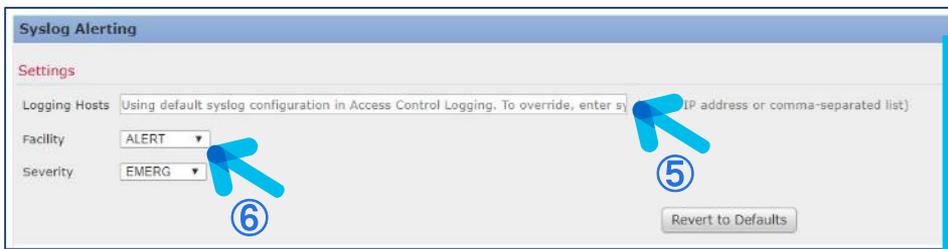
Check boxes below to cause Intrusion Events with the associated Impact Flag to generate alerts.

Impact Flag	Syslog Notification	Email Notification	SNMP Notification
Unknown	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Unknown Target	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Currently Not Vulnerable	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Potentially Vulnerable	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vulnerable	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- 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

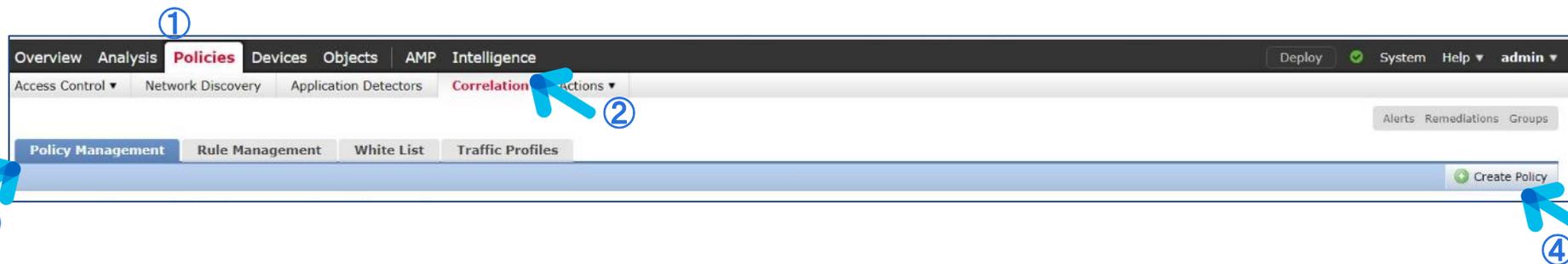
- Intrusion Event設定画面は次のようになる。



- 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

Policy Management Rule Management White List Traffic Profiles

Correlation Policy Information You have unsaved changes Save Cancel

Policy Name: CORRELTION POLICY ②

Policy Description: ①

Default Priority: None ▼

Policy Rules + Add Rules

No Rules Currently Active

- 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

Policy Management Rule Management White List Traffic Profiles

Rule Information

Rule Name: CORRELATION RULE ①

Rule Description:

Rule Group: Ungrouped ▼

Select the type of event for this rule

If and it meets the following conditions:

Rule ②

Snooze: 0 hours

Inactive Periods: There are no defined inactive periods. To add an inactive period, click "Add Inactive Period".

Buttons: Add Inactive Period, Save, Cancel

- 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

Policy Management Rule Management White List Traffic Profiles

Rule Information + Add Connection Tracker + Add User Qualification + Add Host Profile Qualification

Rule Name: CORRELATION RULE
Rule Description:
Rule Group: Ungrouped

Select the type of event for this rule

If an intrusion event occurs and it meets the following conditions:

① + Add condition + Add complex condition

② IOC Tag is Set ③

Rule Options + Add Inactive Period

Snooze
Inactive Periods

④ Save Cancel

- 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



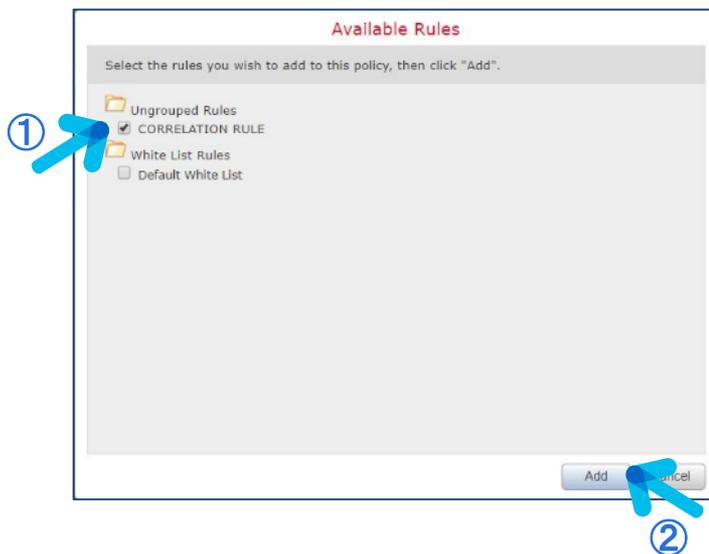
②



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

Policy Management Rule Management White List Traffic Profiles

Correlation Policy Information You have unsaved changes Save Cancel

Policy Name: CORRELATION POLICY

Policy Description: [Empty field]

Default Priority: None

Policy Rules

Rule	Responses	Priority
CORRELATION RULE	This rule does not have any responses.	Default

Add Rules

Responses for CORRELATION RULE

Assigned Responses

Unassigned Responses

SYSLOG-ALERT

Update Cancel

Responses for CORRELATION RULE

Assigned Responses

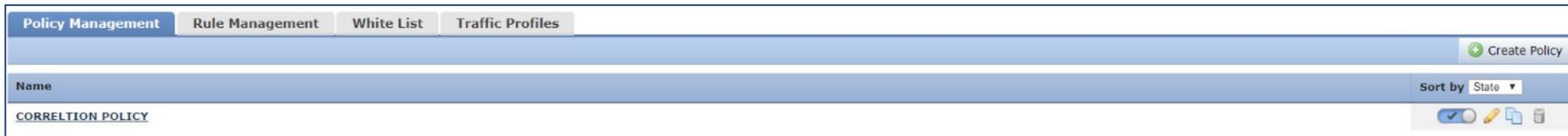
SYSLOG-ALERT

Unassigned Responses

Update Cancel

- 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。

The screenshot shows the Cisco AMP console interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Policies' tab is selected. Below the navigation bar, there are several tabs: 'Access Control', 'Network Discovery', 'Application Detectors', 'Correlation', 'Actions > Alerts', and 'Intrusion Email'. The 'Alerts' link under 'Actions' is highlighted with a blue arrow and a circled '2'. The 'Advanced Malware Protection Alerts' tab is selected in the sub-navigation bar, highlighted with a blue arrow and a circled '3'. The main content area is titled 'Alerts' and contains the following sections:

Alerts

Select alert responses to use for advanced malware detection event alerts. You must click Save after you make your selections.

Syslog:
Email:
SNMP:

Event Configuration

Select the event types for which you want to generate alerts.

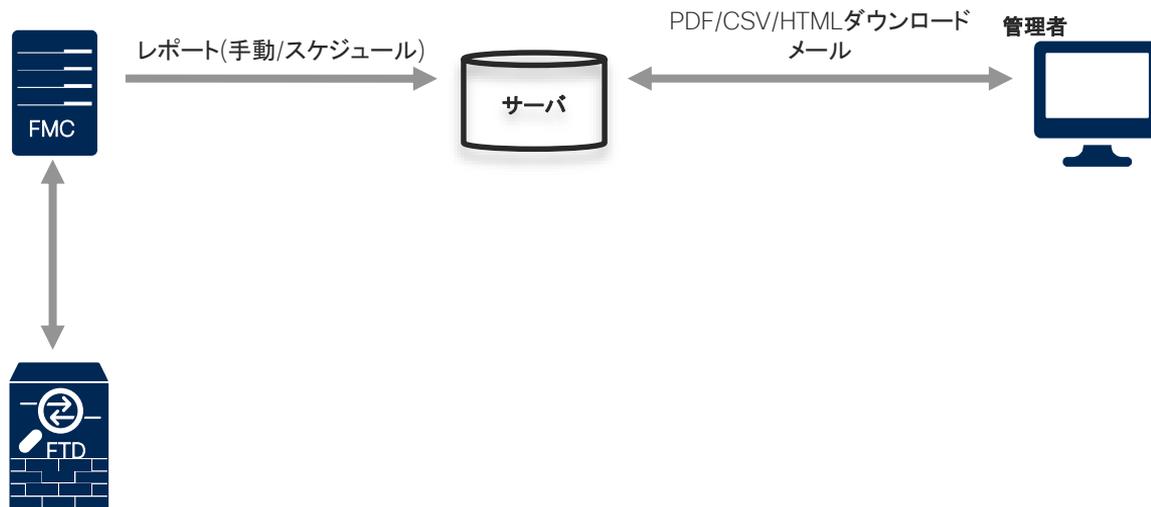
Event	Syslog	Email	SNMP
Retrospective Events	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
All network-based malware events	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- 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

Connection Events (switch workflow)

[Connections with Application Details](#) > [Table View of Connection Events](#)

No Search Constraints ([Edit Search](#))

Jump to... ▾

	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client
↓	2020-04-13 10:43:39		Allow		192.168.1.101		8.8.8.8	USA	inside_zone	outside_zone	65243 / udp	53 (domain) / udp	DNS	DNS client
↓	2020-04-13 10:43:39		Allow		192.168.1.101		172.217.31.130	USA	inside_zone	outside_zone	65244 / udp	443 (https) / udp	DoubleClick	
↓	2020-04-13 10:41:32	2020-04-13 10:41:32	Allow		192.168.1.101		40.74.108.123	JPN	inside_zone	outside_zone	52315 / tcp	443 (https) / tcp	HTTPS	SSL client
↓	2020-04-13 10:41:32	2020-04-13 10:41:32	Allow		192.168.1.101		40.74.108.123	JPN	inside_zone	outside_zone	52316 / tcp	443 (https) / tcp	HTTPS	SSL client
↓	2020-04-13 10:41:32	2020-04-13 10:41:32	Allow		192.168.1.101		8.8.8.8	USA	inside_zone	outside_zone	64935 / udp	53 (domain) / udp	DNS	DNS client
↓	2020-04-13 10:41:32		Allow		192.168.1.101									
↓	2020-04-13 10:41:32		Allow		192.168.1.101									

- Analyticsを選択
- Connections下のEventsを選択
- 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。

The screenshot displays the Cisco ICSA Reporting interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Reporting' section is active, with sub-tabs for 'Dashboards', 'Reporting', and 'Summary'. The 'Report Templates' tab is selected. The 'Report Title' field is set to 'Report of Connection Events' and is highlighted with a blue arrow and a circled '1'. The 'Generate' button is highlighted with a blue arrow and a circled '2'. Below the report title, there are two sections for configuring report sections: 'Connections with Application Details' and 'Table View of Connection Events'. Each section has a 'Table' dropdown set to 'Connection Events', a 'Preset' dropdown set to 'None', a 'Format' selection, a 'Search' dropdown set to 'None', and a 'Fields' list. The 'Section Description' field is set to '\$<Time Window>\$<Constraints>'. The 'Time Window' section has 'Inherit Time Window' unchecked and 'Last hour' checked. The 'Maximum Results' field is set to '10000'. A 'Preview' button is visible at the bottom right of each section.

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。

The screenshot shows the Cisco AMP Reporting interface. The navigation menu includes Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. The main content area is titled 'Reporting' and contains a table of reports. The table has columns for Name, Time Requested, Time Completed, User, Location, and Status. Three reports are listed, all with a status of 'Successfully Processed'. The 'Time Completed' column shows dates and times. Below the table are buttons for Download, Delete, and Move. The storage location is indicated as /var/sf/reports/ (Disk Usage: 11%).

Name	Time Requested	Time Completed	User	Location	Status
<input checked="" type="checkbox"/> Report of Connection Events-20200413014703-383.pdf Reports	2020-04-13 10:47:03	2020-04-13 10:47:09	admin	Local	Successfully Processed
<input checked="" type="checkbox"/> Report of Connection Events-20200413014703-383_csv.zip Reports	2020-04-13 10:47:03	2020-04-13 10:47:10	admin	Local	Successfully Processed
<input checked="" type="checkbox"/> Report of Connection Events-20200413014703-383.zip Reports	2020-04-13 10:47:03	2020-04-13 10:47:08	admin	Local	Successfully Processed

- 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 States)
2020-04-13 10:43:39		Allow	192.168.1.101		172.217.31.130	USA (United States)
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 States)
2020-04-13 10:41:32		Allow	192.168.1.101		8.8.8.8	USA (United States)

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... *

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。

The screenshot displays the 'Report Templates' configuration page in the Palo Alto Networks Reporting tool. The interface includes a top navigation bar with tabs for Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. Below this, there are sections for 'Report Title' (REPORT 20200410) and 'Report Sections'. Two report sections are visible: 'Connections with Application Details' and 'Table View of Connection Events'. Each section has a configuration panel with fields for Table, Preset, Format, Search, and Fields. A toolbar on the right side of the sections contains icons for adding, deleting, and editing sections. Two blue arrows with circled numbers point to these icons: arrow 1 points to the 'Add' icon, and arrow 2 points to the 'Format' field in the first section.

- 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。

The screenshot displays a web application interface for managing report templates. The navigation bar at the top includes 'Overview' (1), 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Reporting' section (2) is active, showing 'Reports' and 'Report Templates' (3). A 'Create Report Template' button is located in the top right. The main content area lists 'Risk Report Templates' (Advanced Malware Risk Report, Attacks Risk Report, Network Risk Report) and 'Templates' (Attack Report: \$<Attack SID>). A toolbar (4) with icons for Generate, Copy, Export, Edit, and Delete is visible on the right side.

- 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 Templates下のは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。

New Task

Job Type ①

Schedule task to run Once Recurring ②

Start On Asia/Tokyo ③

Repeat Every ④ Hours Days Weeks Months

Run At

Repeat On Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Job Name ⑤

Report Template ⑥

Comment

Email Status To [Not available. You must set up your mail relay host.](#)

⑦

- 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。

The screenshot shows a web interface for task scheduling. At the top, there are navigation tabs: Overview, Analysis, Policies, Devices, Objects, AMP, Intelligence, Configuration, Users, Domains, Integration, Updates, Licenses, Health, Monitoring, Tools, and Scheduling. Below this is a calendar for April 2020. The calendar grid shows dates from 1 to 30. A red box highlights the dates 12, 19, and 26, each with a task labeled 'SCHEDULE REPORT'. Below the calendar is a 'Task Details' section, also highlighted with a red box. It contains a table with the following data:

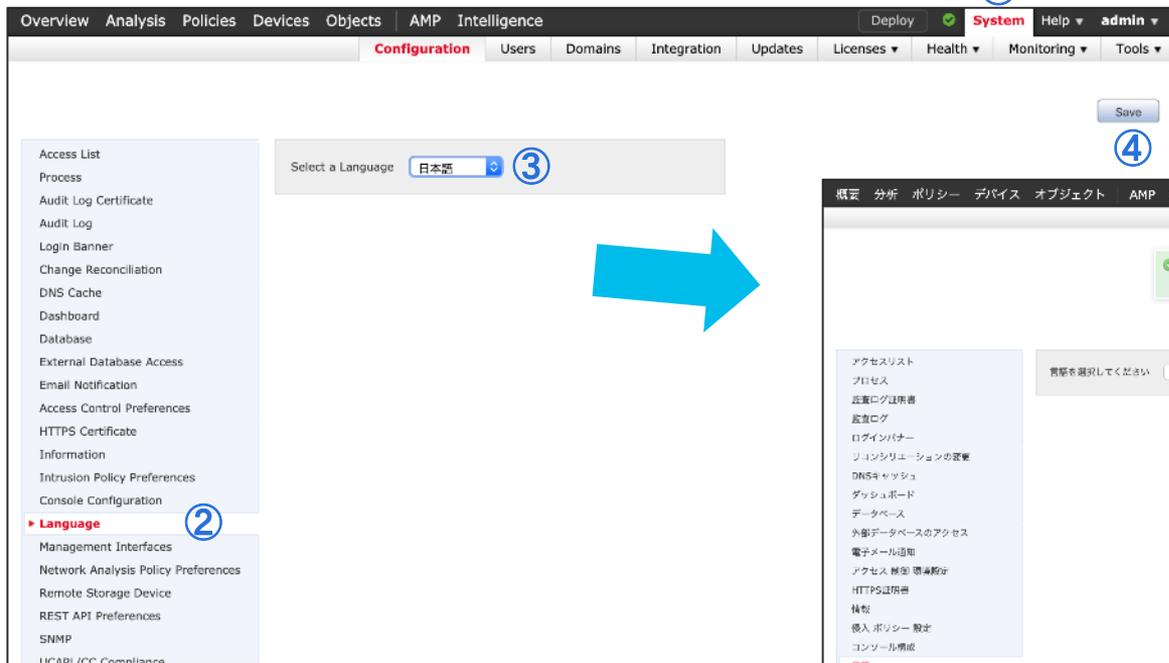
Name	Type	Start Time	Frequency	Last Run Time	Last Run Status	Next Run Time	Creator	Domain
SCHEDULE REPORT	Report	04/11/2020 04:00	Every Week on Sunday	Not run yet	⊕	N/A	admin	Global

- 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)

概要 分析 ポリシー デバイス オブジェクト AMP Intelligence 展開 システム ヘルプ admin

ダッシュボード レポート処理 要約

レポート レポートテンプレート

レポートテンプレートの作成

リスクレポートテンプレート

ネットワークリスクレポート

攻撃リスクレポート

高度なマルウェアリスクレポート

テンプレート

レポート生成

レポート生成情報

ファイル名

タイムウィンドウ Last month

リレーホスト リレーホストが設定されていません!

空のセクション 除外

入力パラメータ

Company Name

Author

Contact

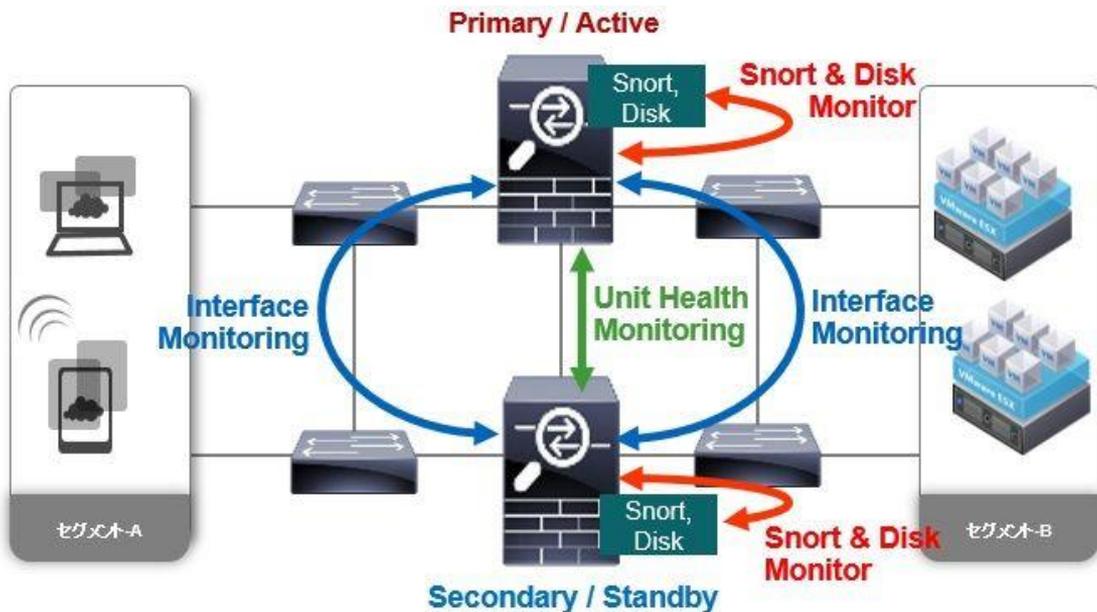
生成 閉じる

※パラメータに日本語を利用可能

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ではヘルスマニタリングとしてインターフェース以外に、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

.132.221

FMCv

.132.220

ESX

Management

.132.222

FTDv01

G0/2 failover 192.168.10.1

G0/2 failover 192.168.10.2

.132.223

FTDv02

G0/1 inside .2

.101

内部LAN

192.168.1.0/24

test PC

管理NW (実態はシスコ検証NW)

外部LAN

192.168.250.0/24

g0/0 グローバルアドレス

ASA

g0/2 .254

Switch

#g1/0/1

#g1/0/2

G0/0 outside .1

G0/1 inside .1

G0/0 outside .2

顧客NW

PAT

PAT



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

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

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

Device Management

List of all the devices currently registered on the Firepower Management Center.

View By: All (4) | **Error (0)** | Warning (0) | Offline (2) | **Normal (2)** | Deployment Pending (2)

Name	Model	Version	Chassis	Licenses	Access Contro...
Ungrouped (2)					
FTDv01 10.71.132.222	Routed	FTD for VMWare 6.4.0.7	N/A	Base, Threat (2 more...)	ACCESS-POLICY
FTDv02 10.71.132.223	Routed	FTD for VMWare 6.4.0.7	N/A	Base, Threat (2 more...)	ACCESS-POLICY

③ 未適用の設定の有無、実行中のタスクの有無も確認

- ① HA構成する2機のヘルス状態が正常であること
- ② モデル、モード、バージョン、ライセンス等が同じであること

ステップ2-1: HA設定 - FTDv01のHAリンクのためのIF有効化

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

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

Device Management

List of all the devices currently registered on the Firepower Management Center.

View By: Group All (4) Error (0) Warning (0) Offline (2) Normal (2) Deployment Pending (2)

Name	Model	Ve...	Chassis	Licenses	Access Control ...
FTDv01 10.71.132.222 - Routed	FTD for VMWare	6.4.0.7	N/A	Base, Threat (2 more...)	ACCESS-POLICY
FTDv02 10.71.132.223 - Routed	FTD for VMWare	6.4.0.7	N/A	Base, Threat (2 more...)	ACCESS-POLICY

- 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 General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

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

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

FTDv01

Cisco Firepower Threat Defense for VMWare

Device Routing **Interfaces** Inline Sets DHCP

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Sta...	IP Address
Diagnostic0/0	diagnostic	Physical			
GigabitEthernet0/0	outside	Physical	outside_zone		192.168.250.1/24(Static)
GigabitEthernet0/1	inside	Physical	inside_zone		192.168.1.1/24(Static)
GigabitEthernet0/2		Physical			
GigabitEthernet0/3		Physical			

Edit Physical Interface

General IPv4 IPv6 Advanced Hardware Configuration

Name: Enabled Management Only

Description:

Mode: None

Security Zone:

Interface ID: GigabitEthernet0/2

MTU: 1500 (64 - 9000)

OK Cancel

ステップ2-2: HA設定 - FTDv02のHAリンクのためのIF有効化

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

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

Device Management

List of all the devices currently registered on the Firepower Management Center.

View By: Group All (4) Error (0) Warning (0) Offline (2) Normal (2) Deployment Pending (2)

Name	Model	Ve...	Chassis	Licenses	Access Control ...	
Ungrouped (2)						
FTDv01 10.71.132.222 - Routed	FTD for VMWare	6.4.0.7	N/A	Base, Threat (2 more...)	ACCESS-POLICY	
FTDv02 10.71.132.223 - Routed	FTD for VMWare	6.4.0.7	N/A	Base, Threat (2 more...)	ACCESS-POLICY	

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

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

FTDv02

Cisco Firepower Threat Defense for VMWare

Device Routing **Interfaces** Inline Sets DHCP

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Sta...	IP Address	
Diagnostic0/0	diagnostic	Physical				
GigabitEthernet0/0		Physical				
GigabitEthernet0/1		Physical				
GigabitEthernet0/2		Physical				
GigabitEthernet0/3		Physical				

- 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 General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

Edit Physical Interface

General IPv4 IPv6 Advanced Hardware Configuration

Name: Enabled Management Only

Description:

Mode: None

Security zone:

Interface ID: GigabitEthernet0/2

MTU: 1500 (64 - 9000)

OK Cancel

ステップ3-1: HA設定 - HAペアの作成

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy 2 System Help admin

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

Device Management

List of all the devices currently registered on the Firepower Management Center.

View By : Group All (4) | Error (0) | Warning (0) | Offline (2) | Normal (2) | Deployment Pending (2)

Name	Model	Version	Chassis	Licenses	Access Control
Ungrouped (2)					
FTDv01 10.71.132.222 - Routed	FTD for VMWare	6.4.0.7	N/A	Base, Threat (2 more...)	ACCESS-POLICY
FTDv02 10.71.132.223 - Routed	FTD for VMWare	6.4.0.7	N/A	Base, Threat (2 more...)	AC

+

- Device
- High Availability
- Stack
- Group

Add High Availability Pair

Name:* FTDv-HA

Device Type: Firepower Threat Defense

Primary Peer: FTDv01

Secondary Peer: FTDv02

Threat Defense High Availability pair will have primary configuration. Licenses from primary peer will be converted to their high availability versions and applied on both peers.

Continue

Cancel

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)

Warning



This operation restarts the Snort processes of primary and secondary devices, temporarily causing traffic interruption.

Do you want to continue?

Do not display this message again

Yes

No

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

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)

Add High Availability Pair

High Availability Link

Interface:* GigabitEthernet0/2
Logical Name:* Failover
Primary IP:* 192.168.10.1
 Use IPv6 Address
Secondary IP:* 192.168.10.2
Subnet Mask:* 255.255.255.0

State Link

Interface:* Same as LAN Failover L
Logical Name:* Failover
Primary IP:* 192.168.10.1
 Use IPv6 Address
Secondary IP:* 192.168.10.2
Subnet Mask:* 255.255.255.0

IPsec Encryption

Enabled
Key Generation: Auto

④ LAN failover link is used to sync configuration, stateful failover link is used to sync application content between peers. Selected interface links and encryption settings cannot be changed later.

Add

Cancel

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

High Availability Pair Added



Configure interface monitoring options to protect the HA pair interfaces. Apply the same health policies to the primary and secondary nodes of the HA pair.

OK

- 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

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

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

Device Management

List of all the devices currently registered on the Firepower Management Center.

View By : Group All (4) | Error (0) | Warning (0) | Offline (2) | Normal (2) | Deployment Pending (2)

Add

Search Device

Name	Model	Ve...	Chassis	Licenses	Access Control ...
Ungrouped (1)					
FTDv-HA High Availability					
FTDv01(Primary, Active) 10.71.132.222 - Routed	FTD for VMWare	6.4.0.7	N/A	Base, Threat (2 more...)	ACCESS-POLICY
FTDv02(Secondary, Standby) 10.71.132.223 - Routed	FTD for VMWare	6.4.0.7	N/A	Base, Threat (2 more...)	ACCESS-POLICY

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)

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

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

FTDv-HA

Cisco Firepower Threat Defense for VMWare

Summary **High Availability** Device Routing Interfaces Inline Sets DHCP

High Availability Configuration

High Availability Link

Interface	State Link
GigabitEthernet0/2	GigabitEthernet0/2
Logical Name: holliver	Logical Name: holliver
Primary IP: 192.168.10.1	Primary IP: 192.168.10.1
Secondary IP: 192.168.10.2	Secondary IP: 192.168.10.2
Subnet Mask: 255.255.255.0	Subnet Mask: 255.255.255.0
IPsec Encryption: Disabled	Statistics

Monitored Interfaces

Interface Name	Active IPv4	Standby IPv4	Active IPv6 - Standby IPv6	Active Link-Local IPv6	Standby Link-Local IPv6	Monitoring
outside	192.168.250.1					<input checked="" type="checkbox"/>
diagnostic						<input type="checkbox"/>
inside	192.168.1.1					<input checked="" type="checkbox"/>

Edit outside

Monitor this interface for failures

IPv4 IPv6

Interface Name: outside

Active IP Address: 192.168.250.1

Mask: 24

Standby IP Address: 192.168.250.2

OK Cancel

Edit inside

Monitor this interface for failures

IPv4 IPv6

Interface Name: inside

Active IP Address: 192.168.1.1

Mask: 24

Standby IP Address: 192.168.1.2

OK Cancel

- 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

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

Dashboards Reporting Summary

FTDv-HA

Cisco Firepower Threat Defense for VMWare

Monitored Interfaces

Interface Name	Active IPv4	Standby IPv4	Active IPv6 - Standby IPv6	Active Link-Local IPv6	Standby Link-Local IPv6	Monitoring
outside	192.168.250.1	192.168.250.2				✓
diagnostic						✓
inside	192.168.1.1	192.168.1.2				✓

Failover Trigger Criteria

Failure Limit	Failure of 1 Interfaces
Peer Poll Time	1 sec
Peer Hold Time	15 sec
Interface Poll Time	5 sec

Interface MAC Addresses

Physical Interface	Active Mac Address	Standby Mac Address
No records to display		

Add Interface Mac Address

Physical Interface:* GigabitEthernet0/0

Active Interface Mac Address:* a200.0a00.00fe

Standby Interface Mac Address:* a200.0a00.00fd

Enter the Mac addresses in hexadecimal format such as 0123.4567.89ab

OK Cancel

Annotations: ① points to the '+' icon in the 'Interface MAC Addresses' table. ② points to the 'Physical Interface' dropdown in the dialog. ③ points to the 'OK' button in the dialog.

- 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

ポートグループの編集: inside

名前	inside
VLAN ID	0
仮想スイッチ	vSwitch2
▼ セキュリティ	
無差別モード	<input checked="" type="radio"/> 承諾 <input type="radio"/> 拒否 <input type="radio"/> vSwitch から継承
MAC アドレス変更	<input checked="" type="radio"/> 承諾 <input type="radio"/> 拒否 <input type="radio"/> vSwitch から継承
偽装転送	<input checked="" type="radio"/> 承諾 <input type="radio"/> 拒否 <input type="radio"/> vSwitch から継承
▶ NIC チーミング	クリックして展開
▶ トラフィック シェーピング	クリックして展開

保存 キャンセル

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 9A0KK2GHVAV
```

```
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)
```

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)

```
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
```

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

The screenshot shows the Cisco FMC Health Monitor interface. The 'Appliance' section lists 'FTDv01'. A red box highlights the 'Advanced Troubleshooting' link. A callout bubble points to it with the text 'Advanced Troubleshootingをクリック'. Below this, the 'Advanced Troubleshooting' window is open, showing the 'Threat Defense CLI' tab selected. A red box highlights this tab, with a callout bubble saying 'Threat Defense CLIをクリック'. In the CLI window, the command 'show' is entered in the 'Command' field, and 'Parameter | failover' is selected in the dropdown. A callout bubble points to this dropdown with the text 'コマンドを選択&入力'. The 'Output' field displays detailed failover status for the primary and secondary hosts. At the bottom of the CLI window, the 'Execute' button is highlighted with a red box, and a callout bubble points to it with the text 'Executeをクリック'.

Health Monitor

Appliance

FTDv01

Generate Troubleshooting Files

Advanced Troubleshooting

Advanced Troubleshootingをクリック

Advanced Troubleshooting

Threat Defense CLI

Threat Defense CLIをクリック

Command: show Parameter | failover

コマンドを選択&入力

Output: 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 9A0KK2GHVAV
Last Failover at: 04:12:14 UTC Mar 31 2020
This host: Primary - Active
Active time: 3690 (sec)
slot 0: ASA v 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: 1814 (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)

Execute

Execute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

FTDv-HA
Cisco Firepower Threat Defense for VMWare High Availability

Summary High Availability Device Routing Interfaces Inline Sets D

General

Name: FTDv-HA

Status: 

Primary Peer: FTDv01(Active)

Secondary Peer: FTDv02(Standby)

Failover History: 

虫眼鏡アイコンを
クリック

Failover History

Time	Device Name	Original State	New State	Reason
04:32:38 UTC Mar 31 2020	FTDv02	Failed	Standby Ready	Interface check
04:32:38 UTC Mar 31 2020				This host:0
04:32:38 UTC Mar 31 2020				Other host:0
04:32:22 UTC Mar 31 2020	FTDv02	Standby Ready	Failed	Interface check
04:32:22 UTC Mar 31 2020				This host:1
04:32:22 UTC Mar 31 2020				single_vf: outside
04:32:22 UTC Mar 31 2020				Other host:0

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

Switch Active Peer
アイコンをクリック

FTDv-HA High Availability									
✓	FTDv01 (Primary, Active) 10.71.132.222 - Routed	FTD for VMWare	6.4.0.7	N/A	Base, Threat (2 more...)	ACCESS-POLICY			
✓	FTDv02 (Secondary, Standby) 10.71.132.223 - Routed	FTD for VMWare	6.4.0.7	N/A	Base, Threat (2 more...)	ACCESS-POLICY			

Switch Active Peer



Are you sure you want to make "FTDv02" the active peer?

Yes

No

Yesをクリック

FTDv-HA High Availability									
✓	FTDv01 (Primary, Standby) 10.71.132.222 - Routed	FTD for VMWare	6.4.0.7	N/A	Base, Threat (2 more...)	ACCESS-POLICY			
✓	FTDv02 (Secondary, Active) 10.71.132.223 - Routed	FTD for VMWare	6.4.0.7	N/A	Base, Threat (2 more...)	ACCESS-POLICY			

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

FTDv-HA High Availability							    
	FTDv01(Primary, Active) 10.71.132.222 - Routed	FTD for VMWare	6.4.0.7	N/A	Base, Threat (2 more...)	ACCESS-POLICY	
	FTDv02(Secondary, Standby) 10.71.132.223 - Routed	FTD for VMWare	6.4.0.7	N/A	Base, Threat (2 more...)	ACCESS-POLICY	

Break HAアイコン
をクリック

Confirm Break

 Breaking the High Availability pair "FTDv-HA" will erase all configuration except the Access Control and Flex Config policy from standby peer. This operation might also restart Snort processes of primary and secondary devices, temporarily causing traffic interruption. Are you sure you want to break the pair?

Force break, if standby peer does not respond

メッセージを確認し問題
なければYesをクリック

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)

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

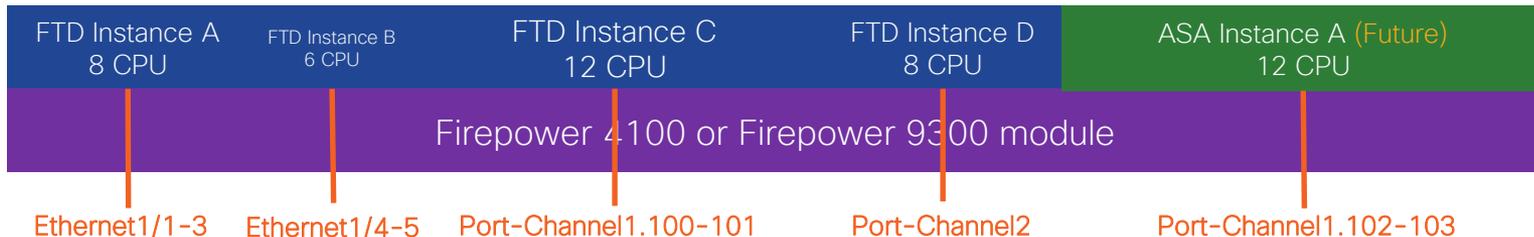
<https://community.cisco.com/t5/-/-/ta-p/3952716>

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	22
Firepower 9300 SM-44	86	36/48/2	750Gb	14	15
Firepower 9300 SM-48 new	94	40/52/2	1.55TB	15	22
Firepower 9300 SM-56 new	110	44/64/2	1.55TB	18	22

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。

Platform Settings

Name	Description	Cores
Default-Small	Auto-created application resource-profile with 6 cpu-cores	6

追加する場合はクリック

デフォルトのプロファイルも存在

クリック

Add Resource Profile

Name: * プロファイル名を記入

Description: 任意で説明を記入

Number of Cores: * コア数を記入(偶数) Range : [6 to 46]

Specify even value for number of cores.

OK Cancel

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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



Add Device

Device Name: デバイス名を記入

Template: FTDを選択

Image Version: バージョンを選択

Instance Type: Containerを選択

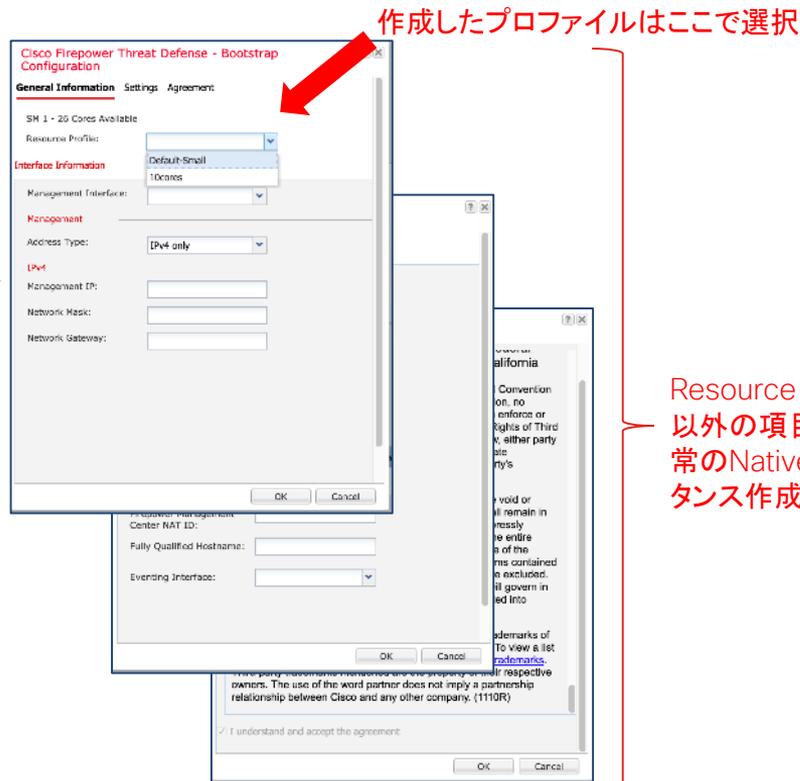
Usage: Standalone Cluster

! Before you add the first container instance, you must reinitialize the security module/engine so that the disk has the correct formatting. You only need to perform this action once.

OK Cancel

※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

Logical Device List

(2 Instances) 57% (26 of 46) Cores Available

作成インスタンス数と使用コア数が表示される

Refresh

Add Device

FTD02

Standalone

Status:ok



Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	6.4.0.102	10cores	10.71.132.226	10.71.135.254	Ethernet1/1	started



FTD01

Standalone

Status:ok



Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	6.4.0.102	10cores	10.71.132.225	10.71.135.254	Ethernet1/1	started



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)

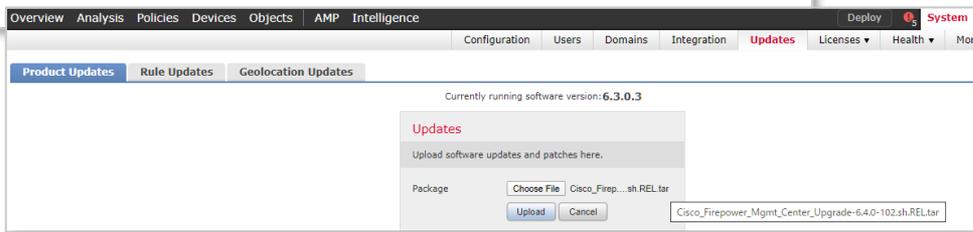
Cisco_Firepower_Mgmt_Center_BIOSUPDATE_640_CJ-12.sh.REL.tar

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

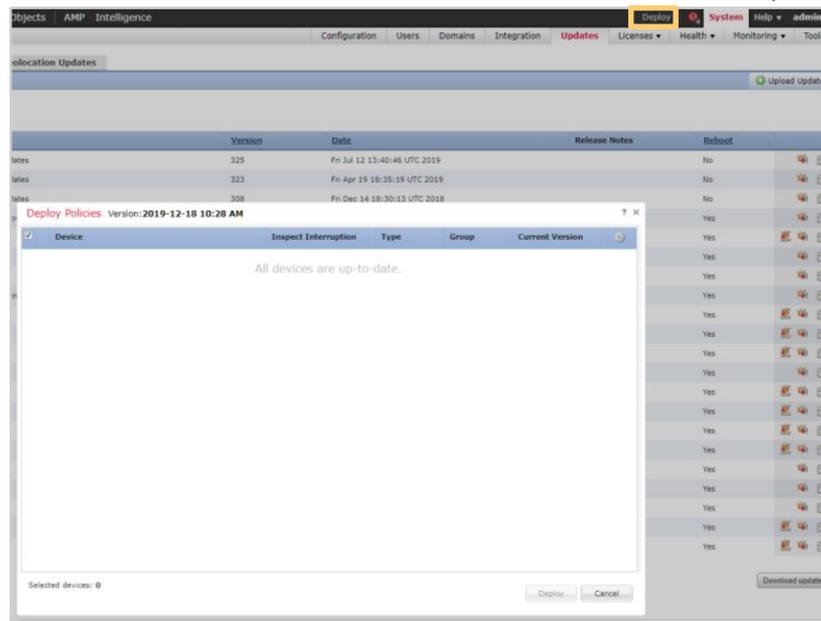
- Primary/Secondary FMCへアップグレードイメージのアップロード
- System > Updates > Upload Update よりイメージをアップロード



Type	Version	Date	Release Notes	Reboot	
Cisco Vulnerability And Fingerprint Database Updates	332	Tue Feb 18 17:18:29 UTC 2020		No	
Cisco Firepower Mgmt Center Patch	6.4.0.7-53	Tue Dec 17 22:30:03 UTC 2019		Yes	
Cisco FTD SSP Patch	6.4.0.7-53	Tue Dec 17 22:12:24 UTC 2019		Yes	
Cisco Firepower Mgmt Center Patch Uninstaller	6.4.0.7-53	Tue Dec 17 22:22:30 UTC 2019		Yes	
Cisco Firepower Mgmt Center Upgrade(v6.2.1 and above)	6.4.0-102	Wed Apr 24 00:04:51 UTC 2019		Yes	

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

1/2

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

The screenshot shows the Cisco FMC interface with the following details:

- Navigation:** Overview, Analysis, Policies, Devices, Objects, AMP, Intelligence, Configuration, Users, Domains, Integration, Updates, Licenses, Health, Monitoring, Tools.
- Sub-Menu:** Cisco CSI, Realms, Identity Sources, High Availability, eStreamer, Host Input Client, Smart Software Satellite, Packet Analyzers.
- Buttons:** Switch Peer Roles, Break HA, Pause Synchronization (highlighted).
- Summary:**
 - Status: Healthy
 - Synchronization: OK
 - Active System: 10.71.253.202 (HA synchronization time: Tue Feb 2020-02-04T06:44:07 UTC)
 - Standby System: 192.168.1.110 (HA synchronization time: Tue Feb 2020-02-04T06:43:10 UTC)
- System Status:**

	Local Active - Primary (10.71.253.202)	Remote Standby - Secondary (192.168.1.110)
Operating System	Fire Linux OS 6.3.0	Fire Linux OS 6.3.0
Software Version	6.3.0.3-77	6.3.0.3-77
Model	Cisco Firepower Management Center 2500	Cisco Firepower Management Center 2500

Warning

This operation may affect critical processes running in the background. Do you want to continue?

Yes No

Warning

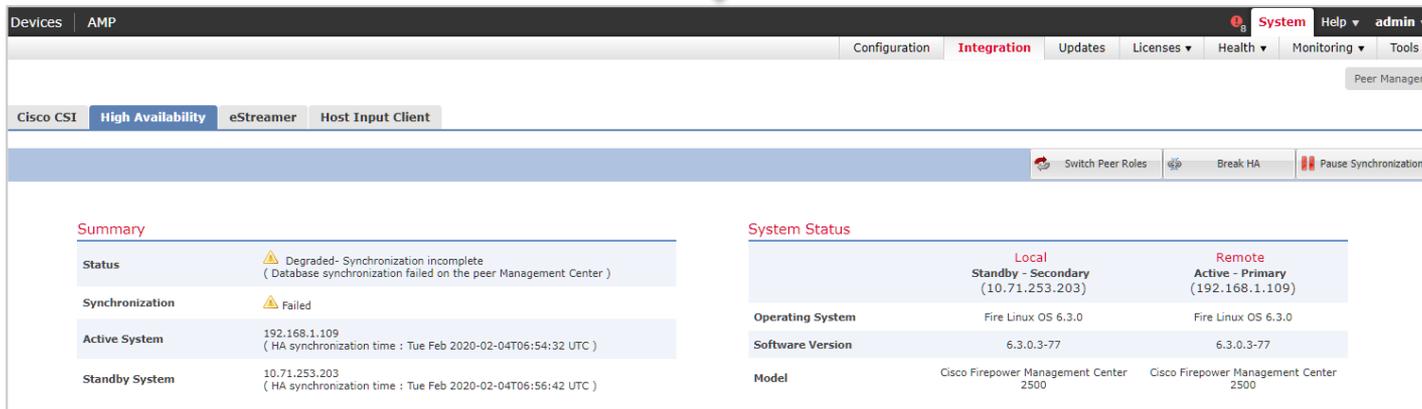
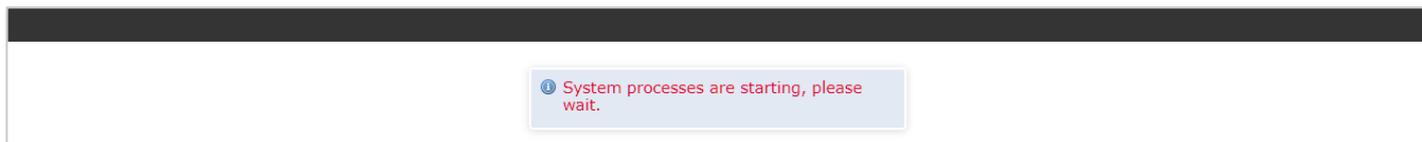
Do you want to pause synchronization?

OK Cancel

※WarningにはYes/OKをクリック

4. HAの同期停止

2/2



The screenshot shows the Cisco AMP High Availability configuration page. The top navigation bar includes 'Configuration', 'Integration', 'Updates', 'Licenses', 'Health', 'Monitoring', and 'Tools'. The main content area is titled 'High Availability' and contains a 'Summary' section and a 'System Status' section.

Summary

Status	Degraded - Synchronization incomplete (Database synchronization failed on the peer Management Center)
Synchronization	Failed
Active System	192.168.1.109 (HA synchronization time : Tue Feb 2020-02-04T06:54:32 UTC)
Standby System	10.71.253.203 (HA synchronization time : Tue Feb 2020-02-04T06:56:42 UTC)

System Status

	Local Standby - Secondary (10.71.253.203)	Remote Active - Primary (192.168.1.109)
Operating System	Fire Linux OS 6.3.0	Fire Linux OS 6.3.0
Software Version	6.3.0.3-77	6.3.0.3-77
Model	Cisco Firepower Management Center 2500	Cisco Firepower Management Center 2500

※Secondary側

5. Secondary FMCのアップグレード

v6.3.0.3 → v6.4.0

1/4

- 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

Devices | AMP

System Help admin

Configuration Integration Updates Licenses Health Monitoring Tools

Product Updates

Upload Update

Currently running software version: 6.3.0.3

Updates

Type	Version	Date	Release Notes	Reboot	
Sourcefire Vulnerability And Fingerprint Database Updates	323	Fri Apr 19 18:35:19 UTC 2019		No	
Cisco Firepower Mgmt Center Upgrade(v6.2.1 and above)	6.4.0-102	Wed Apr 24 00:04:51 UTC 2019		Yes	<input checked="" type="checkbox"/>
Cisco Firepower Mgmt Center Patch Uninstaller	6.3.0.3-77	Thu Apr 25 21:39:14 UTC 2019		Yes	<input type="checkbox"/>

Product Updates

Currently running software version: 6.3.0.3

Selected Update

Type Cisco Firepower Mgmt Center Upgrade(v6.2.1 and above)
Version 6.4.0-102
Date Wed Apr 24 00:04:51 UTC 2019
Release Notes
Reboot Yes

By Group

Ungrouped (1 total)

FMC2K02.cisco.com
10.71.253.203 - Cisco Firepower Management Center 2500 v6.3.0.3

Health Policy
Initial Health Policy 2018-11-20 02:31:17 (Remotely authored by 10.71.253.202)

Launch Readiness Check Cancel

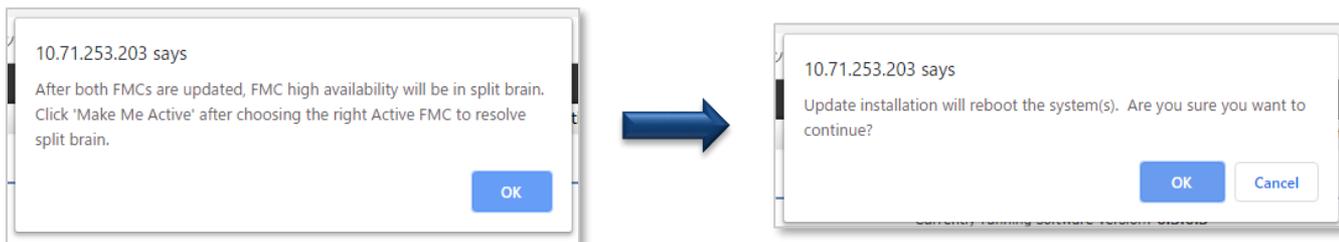
※Health Alertは
ラボ環境により
電源モジュール2
に電源が入って
いないため

5. Secondary FMCのアップグレード

v6.3.0.3 → v6.4.0

2/4

- 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

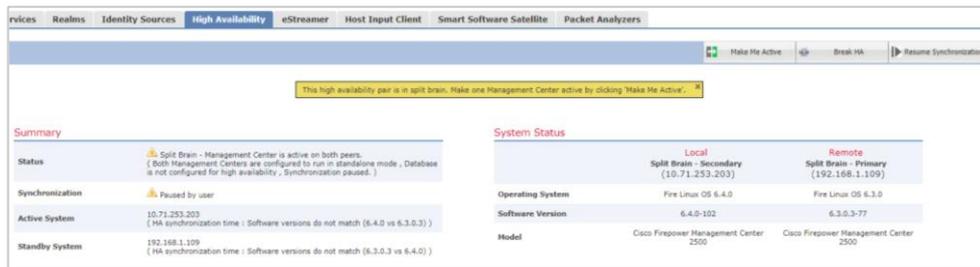
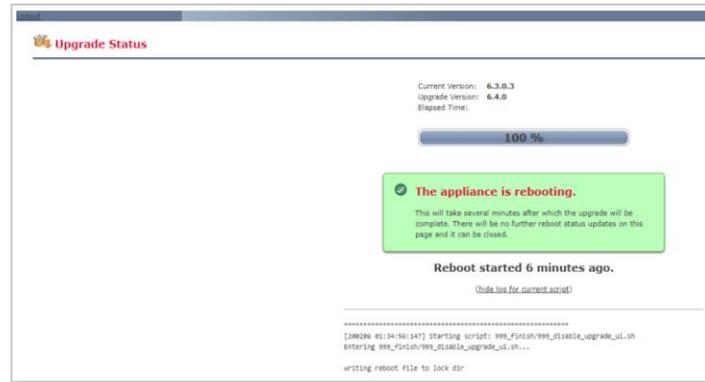
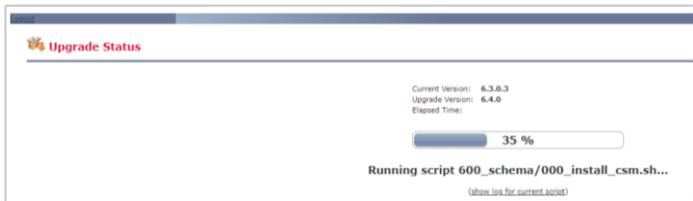


5. Secondary FMCのアップグレード

v6.3.0.3 → v6.4.0

3/4

- ・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



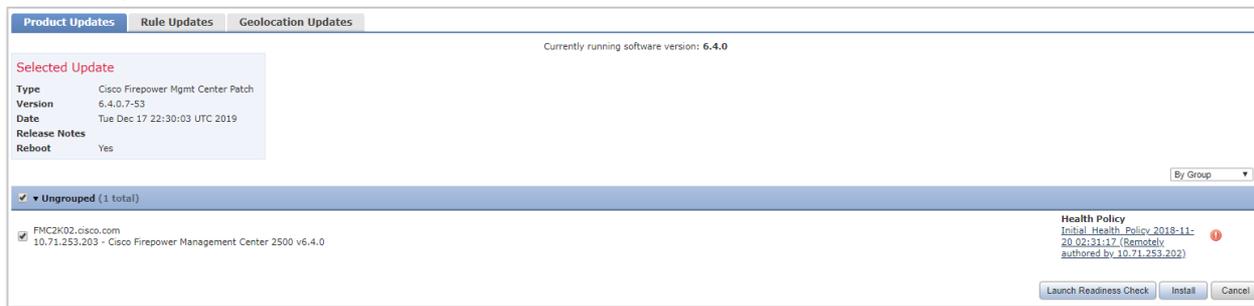
※Upgrade後、HAの状態はSplit Brainとなる

5. Secondary FMCのアップグレード

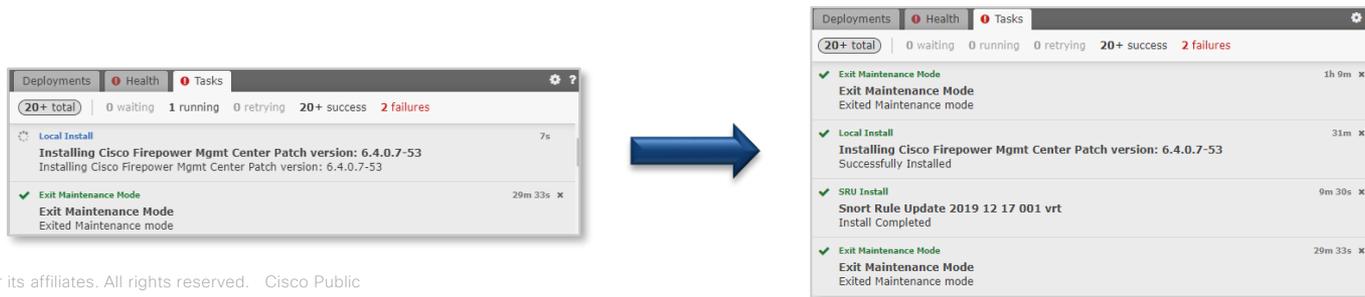
v6.4.0 → v6.4.0.7

4/4

- 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

1/4

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

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools

Product Updates Rule Updates Geolocation Updates Upload Update

Currently running software version: 6.3.0.3

Updates

Type	Version	Date	Release Notes	Reboot	
Sourcefire Vulnerability And Fingerprint Database Updates	325	Fri Jul 12 13:40:46 UTC 2019		No	
Sourcefire Vulnerability And Fingerprint Database Updates	323	Fri Apr 19 18:35:19 UTC 2019		No	
Sourcefire Vulnerability And Fingerprint Database Updates	308	Fri Dec 14 18:30:13 UTC 2018		No	
Cisco Firepower Mgmt. Center Upgrade(v6.2.1 and above)	6.4.0-102	Wed Apr 24 00:04:51 UTC 2019		Yes	
Cisco FTD Patch	6.3.0.3-77	Thu Apr 25 21:27:37 UTC 2019		Yes	Install

Product Updates Rule Updates Geolocation Updates

Currently running software version: 6.3.0.3

Selected Update

Type Cisco Firepower Mgmt. Center Upgrade(v6.2.1 and above)
Version 6.4.0-102
Date Wed Apr 24 00:04:51 UTC 2019
Release Notes
Reboot Yes

By Group

▼ Ungrouped (1 total)

FMC2K01.cisco.com
10.71.253.202 - Cisco Firepower Management Center 2500 v6.3.0.3

Health Policy
Initial: Health_Policy_2018-11-20_02:31:17

Launch Readiness Check Install Cancel

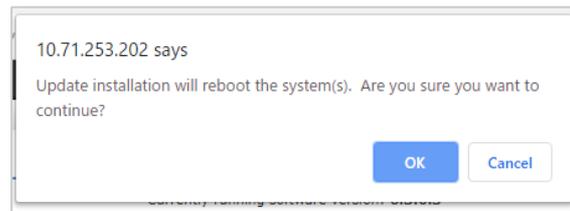
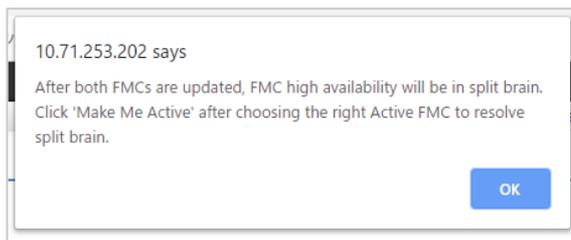
※Health Alertは
ラボ環境により
電源モジュール2
に電源が入って
いないため

6. Primary FMCのアップグレード

v6.3.0.3 → v6.4.0

2/4

- 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

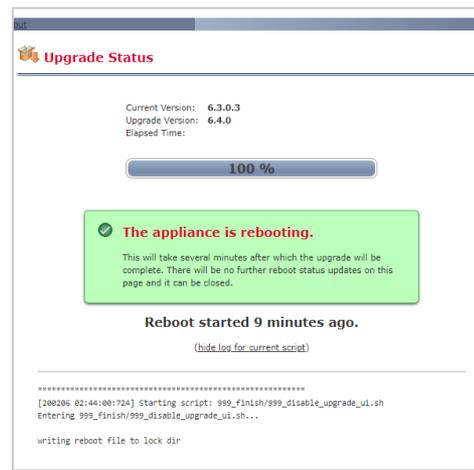
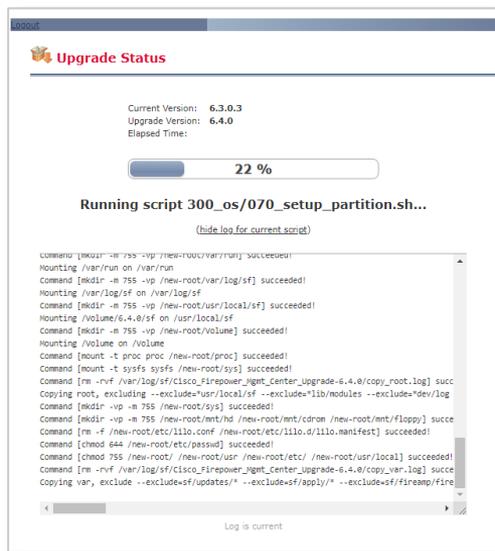


6. Primary FMCのアップグレード

v6.3.0.3 → v6.4.0

3/4

- ・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

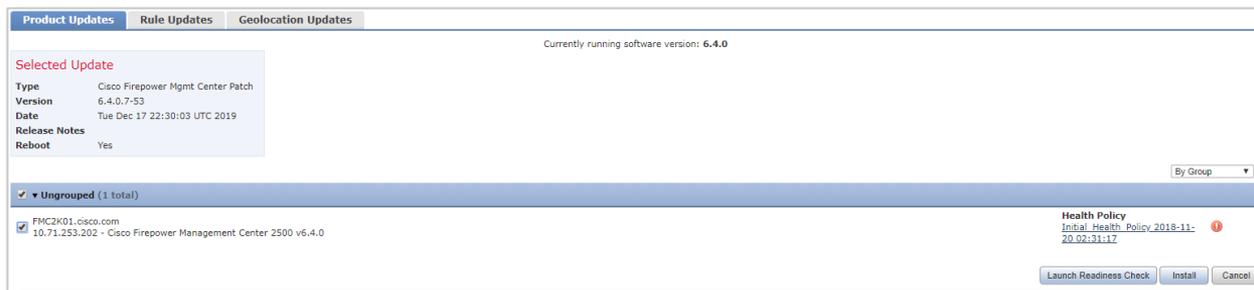


6. Primary FMCのアップグレード

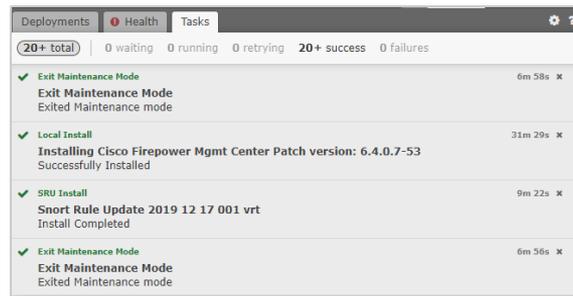
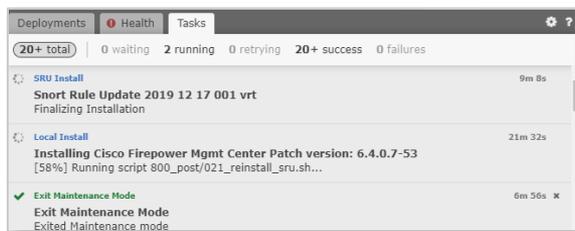
v6.4.0 → v6.4.0.7

4/4

- 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

1/3

- 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
```

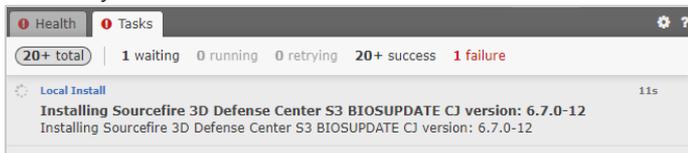
※2.0.13dが現時点のバージョン



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

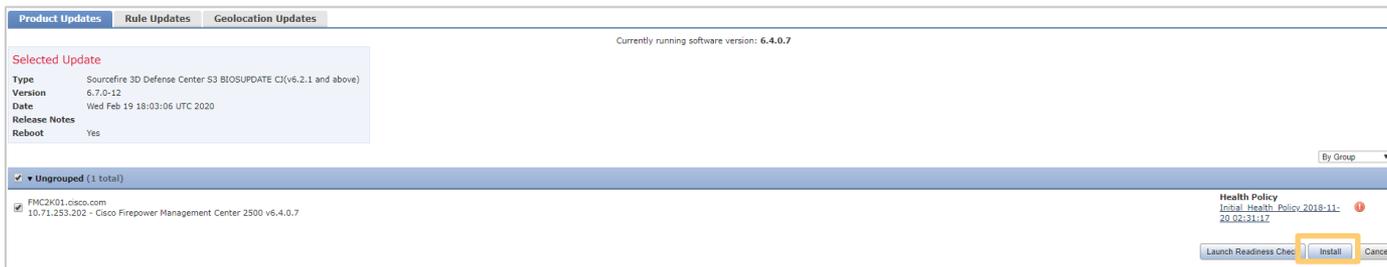
Standby FMC GUI



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

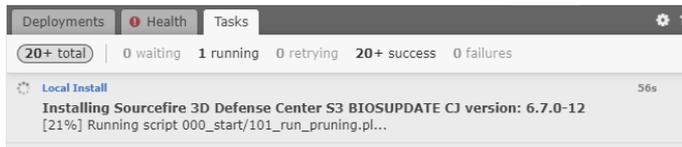


7. Hotfixの適用

3/3

- 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

1/2

- 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

Analysis Policies Devices Objects AMP Intelligence

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools

ices Realms Identity Sources High Availability eStreamer Host Input Client Smart Software Satellite Packet Analyzers

Switch Peer Roles Break HA Resume Synchronization

Summary

Status ⚠ Degraded- Synchronization incomplete
(Both Management Centers are configured to run in standalone mode , Database is not configured for high availability , Synchronization paused.)

Synchronization ⚠ Paused by user

Active System 10.71.253.202
(HA synchronization time : Tue Feb 25 08:33:11 2020)

Standby System 192.168.1.110
(HA synchronization time : HA Upgrade state - not completed)

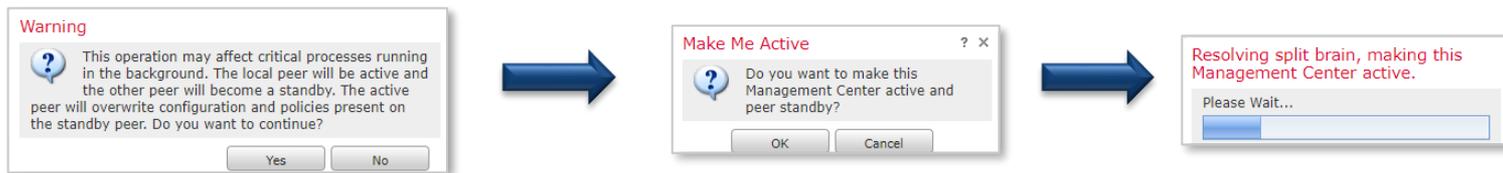
System Status

	Local	Remote
	Active - Primary (10.71.253.202)	Standby - Secondary (192.168.1.110)
Operating System	Fire Linux OS 6.4.0	Fire Linux OS 6.4.0
Software Version	6.4.0.7-53	6.4.0.7-53
Model	Cisco Firepower Management Center 2500	Cisco Firepower Management Center 2500

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

Services Realms Identity Sources **High Availability** eStreamer Host Input Client Smart Software Satellite Packet Analyzers

Switch Peer Roles Break HA Pause

Summary

Status	Healthy
Synchronization	OK
Active System	10.71.253.202 (HA synchronization time : Thu Feb 2020-02-06T05:19:22 UTC)
Standby System	192.168.1.110 (HA synchronization time : Thu Feb 2020-02-06T05:18:59 UTC)

System Status

	Local	Remote
	Active - Primary (10.71.253.202)	Standby - Secondary (192.168.1.110)
Operating System	Fire Linux OS 6.4.0	Fire Linux OS 6.4.0
Software Version	6.4.0.7-53	6.4.0.7-53
Model	Cisco Firepower Management Center 2500	Cisco Firepower Management Center 2500

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>

