



The bridge to possible

Firewall Threat Defense (FMC 管理) Version 7.0 初期セットアップガイド Vol. 2 基本セキュリティポリシー設定編 Rev 2.0

August 2022

シスコシステムズ合同会社

はじめに

- 本ガイドは、Version 7.0 の Firewall Management Center (以下、FMC) 管理の Firewall 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 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。
- 本ガイドは、4部作の Vol. 2 に相当します。

内容に関する保証について

- 本ガイドは、2022年8月現在の情報に基づいており、FTD & FMC のソフトウェアは 7.0.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

.135.254

DNS: 64.104.14.184

ntp.esl.cisco.com

proxy-wsa.esl.cisco.com

10.71.128.0/21

VM Network

.132.194

G0/0 outside .1

FTDv01

test PC2

Management

G0/1 inside .1

.101

.132.204

FMCv

.132.130

ISE-PIC01

.132.220

ESXi

.132.131

内部LAN

192.168.1.0/24

.11

AD01.secvt.jp

test PC1

g0/0 グローバルアドレス

ASA

g0/3 .254

外部LAN

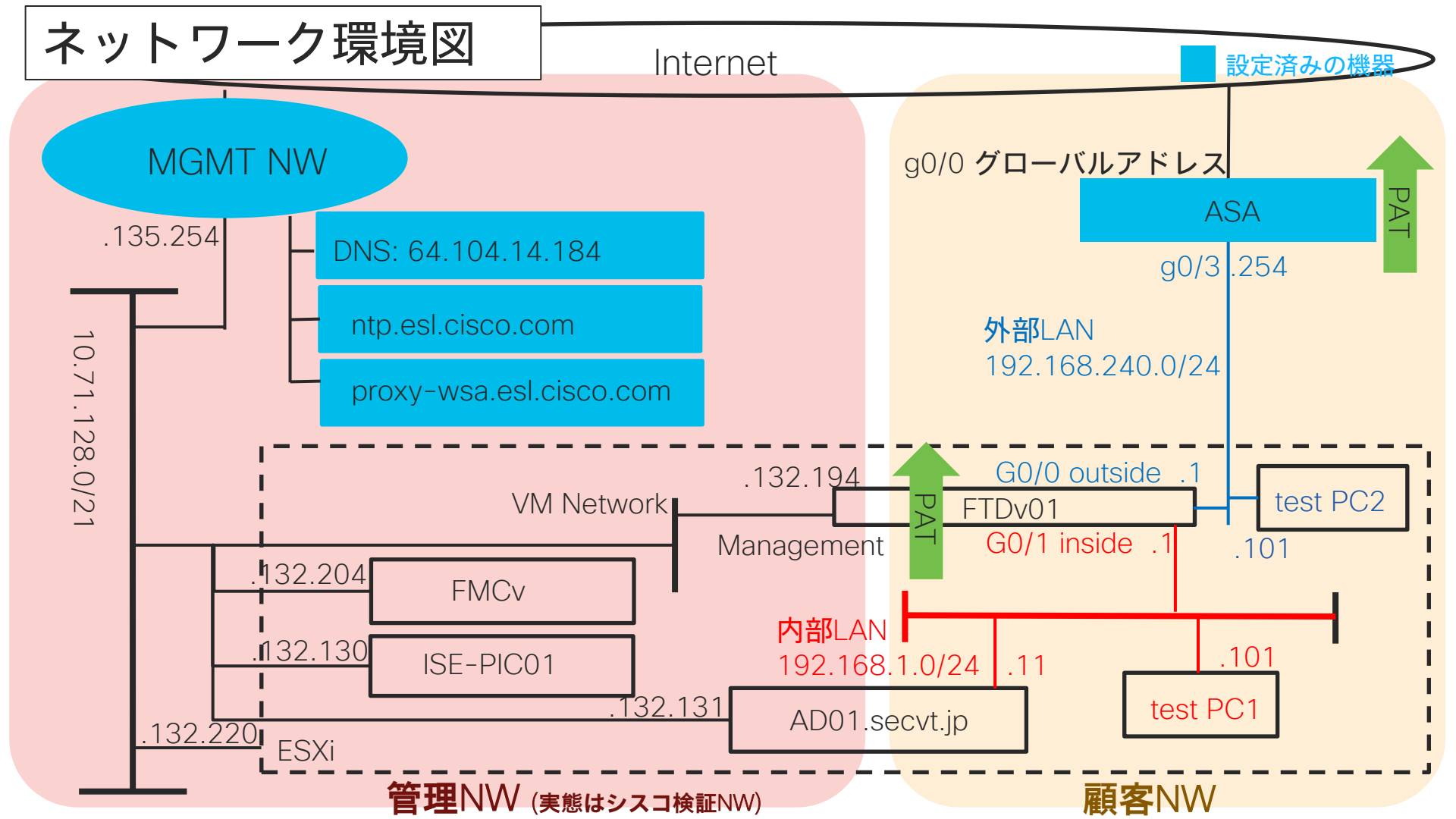
192.168.240.0/24

PAT

PAT

管理NW (実態はシスコ検証NW)

顧客NW



当ガイド (Vol. 2) のシナリオ

- FTD を Routed Firewall と Interface PAT を設定し、inside から outside に向けて通信を可能にする。
- 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 Block list) を利用し、URL カテゴリをロギングするように設定し、ここまでの設定内容に関する動作試験を行う。その後、タイムレンジのアクセスコントロールを設定する。

注意事項

- 製品名称が更新されているが、ソフトウェア名称は旧製品のままで公開されている
- 新名称 ↔ 旧名称
 - Firewall Management Center ↔ Firepower Management Center
 - Firewall Threat Defense ↔ Firepower Threat Defense

Vol.1 (初期インストール編) の目次

1. FMC と FTD のインストール
 - 1-1. FMCv の初期インストール
 - 1-2. FTDv の初期インストール
 - 1-3. (Option) FPR4100/9300 シリーズの初期インストール
 - 1-4. (Option) FPR1000/2100 シリーズの初期インストール
2. FTD と FMC 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. FMC と FTD の Upgrade / Patch インストール

Vol. 2 (基本セキュリティポリシー設定編:当ガイド) の目次

6. Routed Firewall, NAT および Network Discovery の設定
7. Prefilter の設定
8. Intrusion Policy の設定 (Snort3)
9. Malware & File Policy の設定
10. Access Control Policy の設定

Vol. 3 (応用設定編) の目次

11. TLS Decryptionの設定
12. IDFW の設定
13. AnyConnect VPN 接続の設定
14. バックアップの設定とリストアの方法

Vol. 4 (管理・監視・冗長構成編) の目次

- 15. FMC API の利用例
- 16. システム監視
- 17. Syslog・レポート・アラートの設定
- 18. SAL SaaS, SecureX 連携の設定
- 19. 設定ロールバック
- 20. FTD High Availability の設定
- 21. FMC High Availability の設定

6. Routed Firewall、 NAT および Network Discovery

Routed Firewall

Firewall Mode

- FTD では2つのファイアウォールモードをサポート
 - Transparent Firewall Mode: L2 で動作するファイアウォール
 - Routed Firewall Mode: L3 で動作するファイアウォール
- Transparent Firewall Mode
 - Inside/Outside 等の2つ以上のインターフェースをグループ化した“ブリッジグループ”で構成され、L2 ~ L7までのセキュリティ機能を提供
 - Routed Firewall とは異なり、Router Hop とはならないため、デフォルトゲートウェイとしての設定は不可 (ただし、ブリッジグループを管理するための管理 IP (BVI) の設定は必須)
- Routed Firewall Mode (本章で記載)
 - ネットワークにてRouter Hop として動作。それぞれのインターフェースは異なるサブネットで構成されルーティングを行う

Routed Firewall Mode

- FTD でサポートされるルーティングおよび機能
 - Static Routing: Static Route, null0 ルーティング
 - Dynamic Routing: OSPFv2,v3 / RIPv1,v2 / BGP (EIGRP は Flex Config のみ)
EIGRP は Version 7.2 で FMC からの設定が可能になる予定
 - Multicast Routing
 - VRF
 - Route map
- HA 構成時の Routing Table Update
 - RIB (Routing Information Base) テーブルはルートの更新時に Standby Unit にも同期され、常に最新のルーティング情報が Standby Unit にもレプリケーションされる

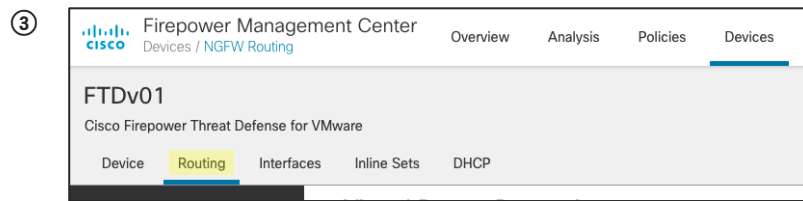
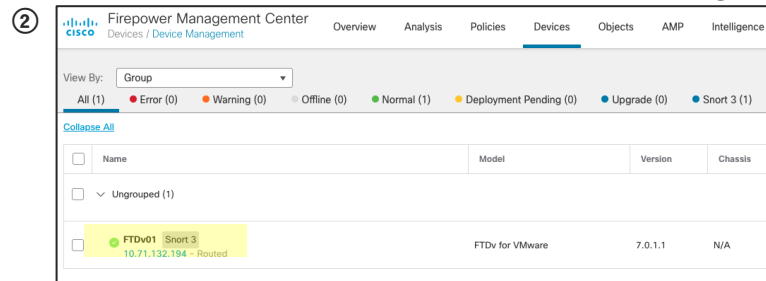
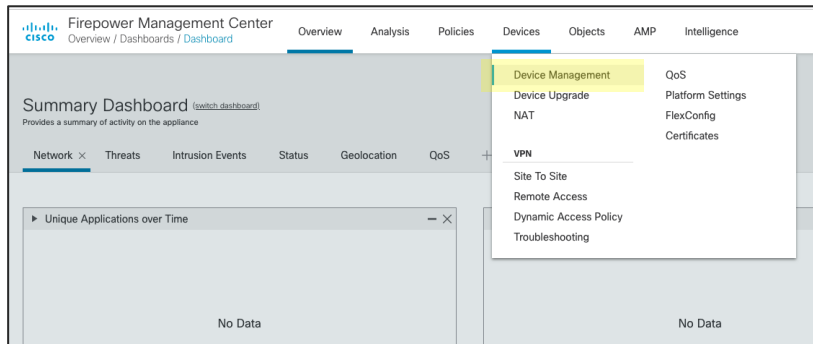
設定手順 (例: Static Route)

1/5



- データ通信用 Default Gateway の設定
- 設定要件: FTD の Default Gateway は ASA 192.168.240.254 とする

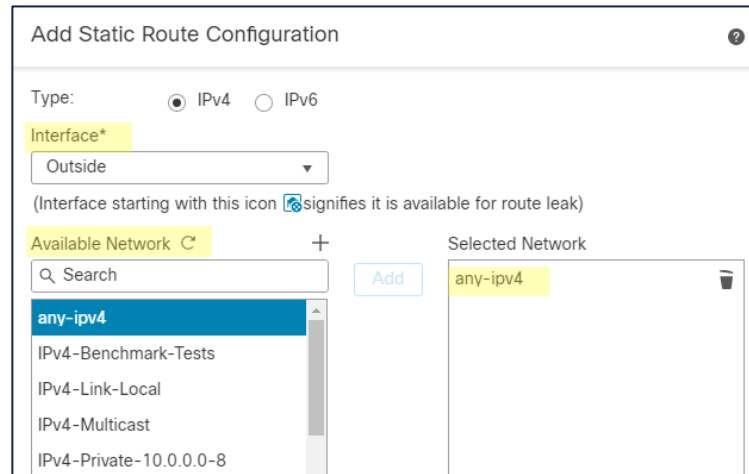
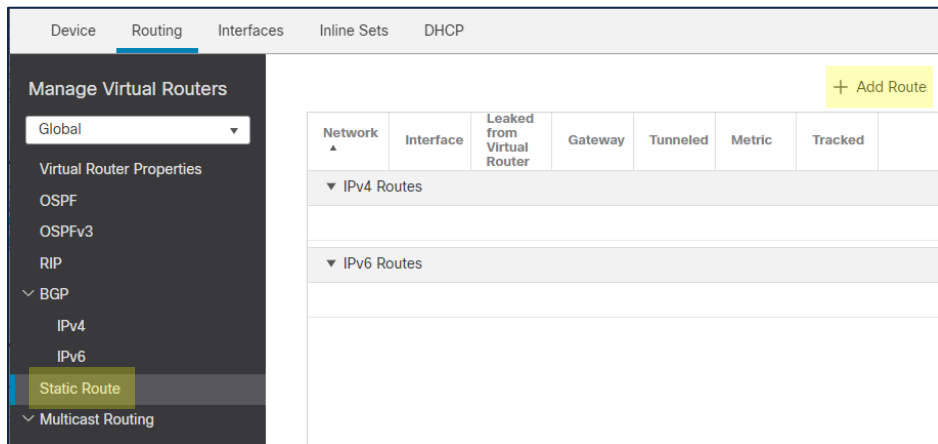
① 1. FMC: Devices > Device Management > FTDv01(管理デバイス名) > Edit > Routing



設定手順 (例: Static Route)

2/5

- データ通信用 Default Gateway の設定
 2. Static Route の追加: Static Route > + Add Route を選択
 3. 適用するルート of インターフェース選択およびネットワークの選択:
Add Static Route Configuration > Interface & Available Network



設定手順 (例: Static Route)

3/5

- データ通信用 Default Gateway の設定

- Gateway の設定 (a または b)

- Network Object の作成: Gateway > + > 設定後 Save

- Network Object の選択(a. が作業済み):

- a. で作成したオブジェクトを Drop down メニューから選択 > OK

b.

Gateway*

asa_default_gw +

asa_default_gw

1

(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:

Cancel OK

Gateway*

+ a.

New Network Object

Type:

Interface: Outsideside

Name: asa_default_gw

Description: Default GW on ASA

Network: Host Range Network FQDN

IPV4-Be: 192.168.240.254

IPV4-Lit

IPV4-Mi

IPV4-Pr

IPV4-Pr

Allow Overrides

Cancel Save

Gateway* +

設定手順 (例: Static Route)

4/5

- データ通信用 Default Gateway の設定

5. 設定の保存: Save ボタンをクリックし、Deploy > デバイスの選択 > Deploy を実行

The screenshot shows the Cisco FTDv01 configuration interface. The top navigation bar includes 'Device', 'Routing', 'Interfaces', 'Inline Sets', and 'DHCP'. The 'Routing' tab is active, and the 'Static Route' option is selected in the left sidebar. The main area displays a table of routes:

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
IPv4 Routes						
any-ipv4	Outside	Global	asa_default_gw	false	1	
IPv6 Routes						

Below the table, a deployment dialog is open. It shows the 'Deploy' button and a search bar. The search results table is as follows:

Device	Modified by	Inspect Interru...	Type	Group	Last Deploy Time	Preview	Status
<input checked="" type="checkbox"/>	FTDv01	System, fmcadmin	FTD		Mar 15, 2022 2:2...		Pending

設定手順 (例: Static Route)

5/5

- FTD CLI 結果

```
> show running-config | include route
route Outside 0.0.0.0 0.0.0.0 192.168.240.254 1

> show route

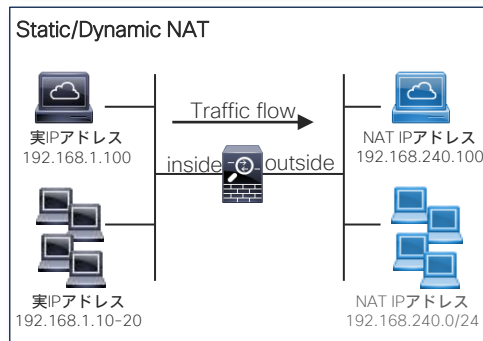
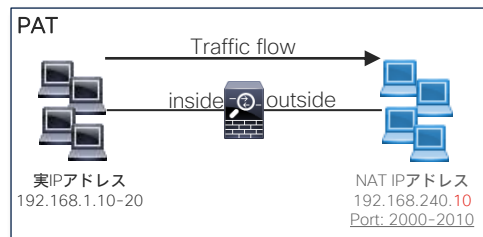
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-
2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 192.168.240.254 to network 0.0.0.0

S*      0.0.0.0 0.0.0.0 [1/0] via 192.168.240.254, Outside
```

NAT

NAT 種類および変換方式

- NAT 種類
 - NAT: 実 IP アドレスを NAT (マップされた) アドレスに変換し、実 IP アドレスを変換する方法 (Network Address Translation)
 - PAT: 1つの NAT アドレスに複数のポートを割り当て、複数の IP アドレスを変換する方法 (Port Address Translation)
- NAT タイプ
 - Static NAT: 1対1または多対多の固定 NAT アドレス変換方式。双方向 (NAT アドレスに対しても) アクセス可
 - Dynamic NAT: IP アドレスプールから先着順に NAT アドレスを割り当てる方法。実ホストからのみアクセス可




FTD での NAT (Auto NAT / Manual NAT)

- NATの設定方には Auto NAT、Manual NAT の2種類ある
 - Auto NAT (Cisco 推奨)
 - Network Object を利用し実 IP Address を NAT アドレスへ変換する最もシンプルな NAT 定義
 - Manual NAT
 - Source と Destination のアドレス変換を一括 (1ルール) で定義
- Auto NAT / Manual NAT の違い
 - Auto NAT は Source または Destination 毎に NAT ルールを作成。それぞれの NAT ルールを組み合わせることで Source / Destination の一つのルールとして結びつけることができない
 - Manual NAT は単一のルールにて Source / Destination 両方のアドレスに対して NAT ルールを適用することができる。そのため、Source A / Destination A の NAT ルールと、Source A / Destination B の NAT ルールのように Source A に対して複数の NAT ルールを適用することができる

FTD での NAT (Auto NAT / Manual NAT)

- NAT 実施順序

- NAT の順序は以下3つのカテゴリに分けられ、これらのカテゴリを順番に評価し、最初に一致したルールを適用する (※Auto NAT に関しては評価の仕方が異なる)

- 
1. NAT Rules Before (Manual NAT)
 2. Auto NAT Rules (Auto NAT)
 3. NAT Rules After (Manual NAT)

- Auto NAT 実施順序

- 
1. Static NAT Rule が Dynamic NAT Rule の前に評価される
 2. 実 IP アドレスの数が少ない方が実 IP アドレスの数が多い方よりも先に評価される
 3. もし、実 IP アドレスの数が他の Auto NAT Rule と同じ場合、数の低い IP アドレスが先に評価される (例: 192.168.1.100 は 192.168.2.1 よりも低い数)
 4. もし、実 IP アドレスが同じ場合、Object 名の名前でアルファベット順に評価される

NAT 設定手順

- NAT ポリシーの作成
- NAT ルールの追加
 - Auto NAT または Manual NAT Rule 選択
 - NAT タイプ (Static NAT または Dynamic NAT) の選択
 - NAT 対象のインターフェースを選択
 - NAT 対象のホスト、レンジ、ネットワークなどを設定
 - NAT アドレス (変換後のアドレス) を設定
- Access Control Policy にて対象トラフィックのアクセスを許可する
(※ ACP の設定方法は 10章にて記載)

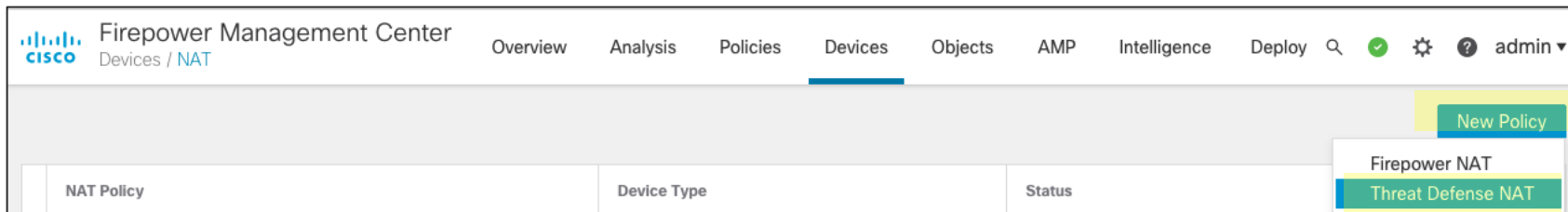
NAT 設定手順 (Auto / Manual NAT 共通)

1/2

- NAT ポリシーの作成
Devices > NAT を選択



New Policy > Threat Defense NAT を選択 (Firepower NAT は NGIPS 専用機器 NAT となるため、FTD での NAT 設定はこちらを選択)



NAT 設定手順 (Auto / Manual NAT 共通)

2/2

- New Policy 画面にてポリシー名
NAT ポリシーを適用するデバイス
を選択する

例

Name: FTDv01_NAT_Policy

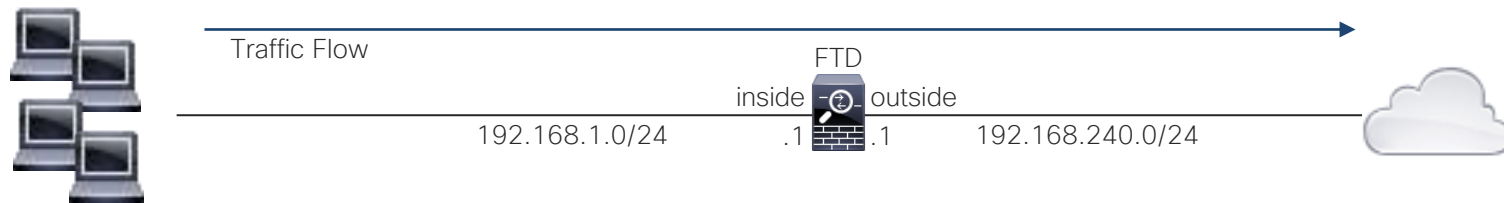
Description: For FTDv01

Targeted Devices: FTDv01

The screenshot shows the 'New Policy' configuration window. The 'Name' field is set to 'FTDv01_NAT_Policy' and the 'Description' field is set to 'For FTDv01'. Under 'Targeted Devices', there is a search bar with the text 'Search by name or value'. Below the search bar, a list of 'Available Devices' contains 'FTDv01', which is highlighted. An 'Add to Policy' button is positioned to the right of the list. To the right of the 'Available Devices' list is a 'Selected Devices' list, which contains 'FTDv01'. At the bottom of the window, there are 'Cancel' and 'Save' buttons.

NAT 設定手順 (Auto NAT 設定例)

1/7

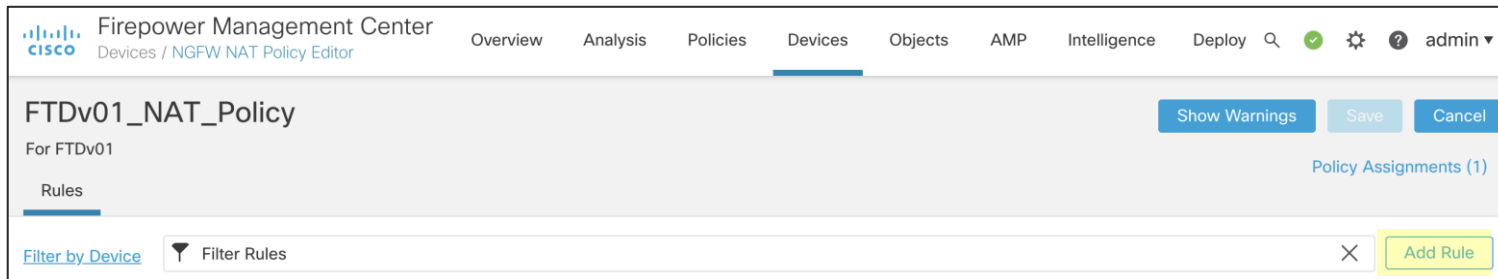


- 設定要件: Inside セグメントにあるすべてのホストが outside セグメントへアクセスする際、FTD の outside インターフェースのアドレスに変換する
 - Source Address: 192.168.1.0/24 (Dynamic NAT)
 - Destination Address (NAT Address): 192.168.240.1 (outside interface ip)

NAT 設定手順 (Auto NAT 設定例)

2/7

- Add Rule を選択し、新規 NAT Rule を追加する



Firepower Management Center
Devices / NGFW NAT Policy Editor

Overview Analysis Policies Devices Objects AMP Intelligence Deploy

FTDv01_NAT_Policy
For FTDv01

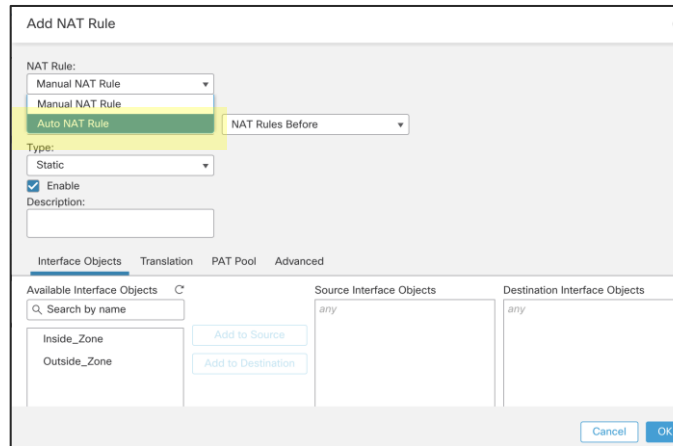
Show Warnings Save Cancel

Policy Assignments (1)

Rules

Filter by Device Filter Rules Add Rule

- NAT Rule に Auto NAT を選択



Add NAT Rule

NAT Rule:
Manual NAT Rule
Manual NAT Rule
Auto NAT Rule NAT Rules Before

Type:
Static

Enable

Description:

Interface Objects Translation PAT Pool Advanced

Available Interface Objects C Source Interface Objects Destination Interface Objects

Search by name any any

Inside_Zone Add to Source

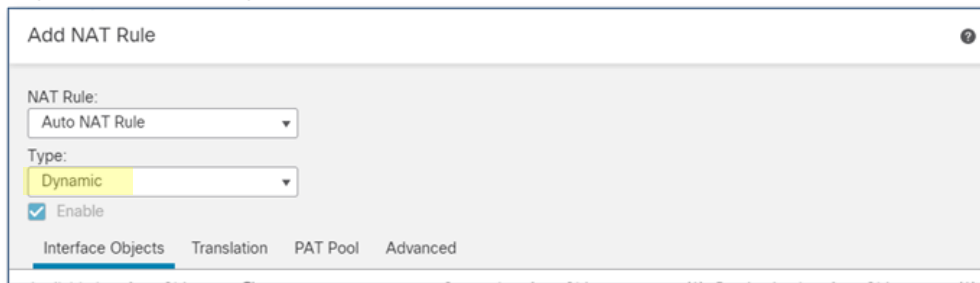
Outside_Zone Add to Destination

Cancel OK

NAT 設定手順 (Auto NAT 設定例)

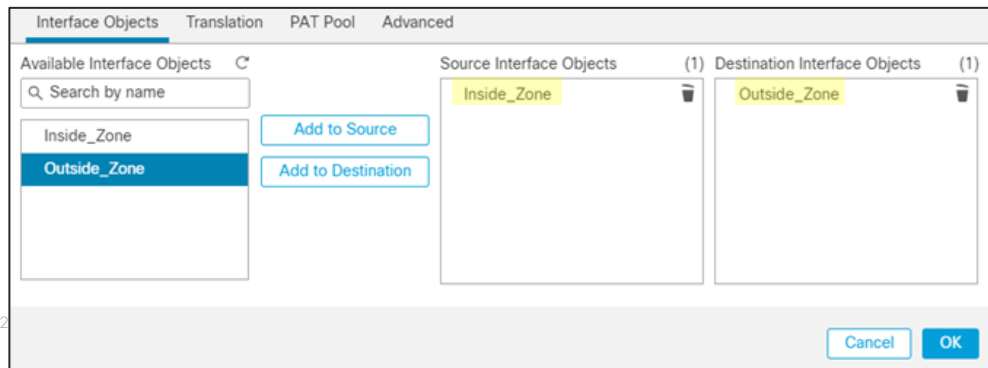
3/7

- Type に Dynamic を選択



The screenshot shows the 'Add NAT Rule' dialog box. The 'NAT Rule' dropdown is set to 'Auto NAT Rule'. The 'Type' dropdown is set to 'Dynamic'. The 'Enable' checkbox is checked. The 'Interface Objects' tab is selected.

- Interface Objects で NAT 対象のインターフェースゾーンを選択



The screenshot shows the 'Interface Objects' tab in the NAT rule configuration. The 'Available Interface Objects' list contains 'Inside_Zone' and 'Outside_Zone'. 'Outside_Zone' is selected. The 'Source Interface Objects' list contains 'Inside_Zone'. The 'Destination Interface Objects' list contains 'Outside_Zone'.

NAT 設定手順 (Auto NAT 設定例)

4/7

- Translation タブに移動し、NAT 対象のネットワークを選択する。予め Network Object を作成している場合は、Original Source のドロップダウンメニューより該当ネットワークを選択。未作成の場合、Add ボタンにて Network Object を作成する (New Network Object)

Interface Objects Translation PAT Pool Advanced

Original Packet Translated Packet

Original Source:* Translated Source:

Address

Original Port: Translated Port:

TCP

Add



New Network Object

Name

192.168.1.0_inside_hosts

Description

Network

Host Range Network FQDN

192.168.1.0/24

Allow Overrides

Cancel Save

- Save ボタンにて設定を保存する

NAT 設定手順 (Auto NAT 設定例)

5/7

- Original Source に、NAT 対象のオブジェクトを選択
- Translated Source に、NAT アドレスとなる Destination Interface IP を選択
- OK を選択し、設定を適用する (PAT Pool、Advanced タブは本前提では設定対象外)

The screenshot shows the 'Translation' tab of the NAT configuration dialog. The 'Original Packet' section has 'Original Source:*' set to a dropdown menu. The dropdown list is open, showing several options: '192.168.1.0_inside_hosts' (highlighted in green), 'asa_default_gw', 'IPv4-Benchmark-Tests', 'IPv4-Link-Local', 'IPv4-Multicast', 'IPv4-Private-10.0.0.0-8', and 'IPv4-Private-172.16.0.0'. The 'Translated Packet' section has 'Translated Source:' set to 'Address'.

The screenshot shows the 'Translation' tab of the NAT configuration dialog. The 'Original Packet' section has 'Original Source:*' set to '192.168.1.0_inside_hosts' and 'Original Port:' set to 'TCP'. The 'Translated Packet' section has 'Translated Source:' set to 'Destination Interface IP' (highlighted in green) and 'Translated Port:' set to 'Address'. At the bottom right, there are 'Cancel' and 'OK' buttons.

NAT 設定手順 (Auto NAT 設定例)

6/7

- NAT ポリシーにルールを追加後、Save ボタンで設定を保存

FTDv01_NAT_Policy You have unsaved changes Show Warnings Save Cancel

For FTDv01 Policy Assignments (1)

Rules

[Filter by Device](#) × Add Rule

#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Packet			Translated Packet			Options	
					Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services		
∨ NAT Rules Before												
∨ Auto NAT Rules												
#	✕	Dynamic	Inside_Zone	Outside_Zone	📄	192.168.1.0_inside_hosts	📄	Interface			Dns:false	🗑️
∨ NAT Rules After												

NAT 設定手順 (Auto NAT 設定例)

7/7

- FTD CLI 結果

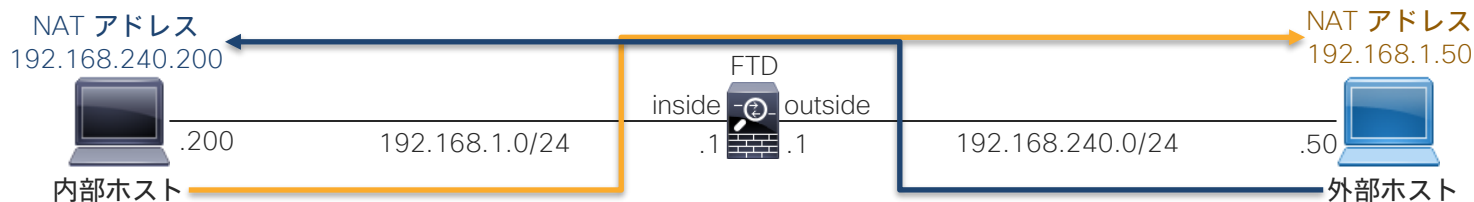
```
> show running-config
object network 192.168.1.0_inside_hosts
 nat (Inside,Outside) dynamic interface

object network 192.168.1.0_inside_hosts
 nat (Inside,Outside) dynamic interface

> show nat detail
Auto NAT Policies (Section 2)
1 (Inside) to (Outside) source dynamic 192.168.1.0_inside_hosts interface
 translate_hits = 0, untranslate_hits = 0
 Source - Origin: 192.168.1.0/24, Translated: 192.168.240.1/24
```


NAT 設定手順 (Manual NAT 設定例)

1/10



- 設定要件: inside セグメント 192.168.1.200 のホストは outside セグメントへのアクセスの際、192.168.240.200 の NAT アドレスに変換。かつ、outside セグメント 192.168.240.50 のホストは 192.168.1.50 の NAT アドレスに変換。これにより、内部ホストおよび外部ホスト間の通信は NAT アドレスにてやり取りを行う。(お互い同セグメントのホストと認識し通信が可能)※
 - 内部ホスト
Source Address: 192.168.1.200
Destination Address (NAT Address): 192.168.240.200
 - 外部ホスト
Source Address: 192.168.240.50
Destination Address (NAT Address): 192.168.1.50

NAT 設定手順 (Manual NAT 設定例)

2/10

- Add Rule にて新規 NAT ルールを追加する

Add NAT Rule

NAT Rule:
Manual NAT Rule

Insert:
In Category NAT Rules Before

Type:
Static

Enable

Description:

Interface Objects Translation PAT Pool Advanced

- NAT Rule は Manual NAT Rule を選択
- Insert はどのカテゴリに NATを追加するかを決定 → NAT Rules Before を選択
- Type は Static を選択

NAT 設定手順 (Manual NAT 設定例)

3/10

- Interface Objects タブにて NAT 対象のインターフェースの選択

The screenshot displays the NAT configuration interface with the 'Interface Objects' tab selected. The interface is divided into three main sections:

- Available Interface Objects:** A search box labeled 'Search by name' is at the top. Below it, a list contains 'Inside_Zone' and 'Outside_Zone'. 'Outside_Zone' is highlighted in blue, indicating it is selected. To the right of this list are two buttons: 'Add to Source' and 'Add to Destination'.
- Source Interface Objects:** A box labeled '(1) Source Interface Objects' containing 'Inside_Zone' highlighted in yellow. A trash icon is visible to the right of the item.
- Destination Interface Objects:** A box labeled '(1) Destination Interface Objects' containing 'Outside_Zone' highlighted in yellow. A trash icon is visible to the right of the item.

NAT 設定手順 (Manual NAT 設定例)

4/10

- Translation タブにて NAT 対象ホストを設定
 - Original Source に inside 側ホストの実 IP アドレスで新規オブジェクトを作成し、適用

The screenshot shows the 'Translation' tab in a configuration interface. It is divided into two columns: 'Original Packet' and 'Translated Packet'. Under 'Original Packet', there are four rows of fields: 'Original Source:*' (with a dropdown menu and a '+' button), 'Original Destination:' (with a dropdown menu and a '+' button), 'Original Source Port:' (with a dropdown menu and a '+' button), and 'Original Destination Port:' (with a dropdown menu and a '+' button). Under 'Translated Packet', there are four rows of fields: 'Translated Source:' (with a dropdown menu and a '+' button), 'Translated Destination:' (with a dropdown menu and a '+' button), 'Translated Source Port:' (with a dropdown menu and a '+' button), and 'Translated Destination Port:' (with a dropdown menu and a '+' button). The 'Original Source:*' field is highlighted in yellow.

The screenshot shows the 'New Network Object' dialog box. It has a title bar with a question mark icon. The 'Name' field contains 'in_host1' and is highlighted in yellow. The 'Description' field is empty. The 'Network' section has four radio buttons: 'Host' (selected), 'Range', 'Network', and 'FQDN'. Below the radio buttons, there is a text input field containing '192.168.1.200' and highlighted in yellow. There is a checkbox labeled 'Allow Overrides' which is currently unchecked. At the bottom right, there are two buttons: 'Cancel' and 'Save'.

NAT 設定手順 (Manual NAT 設定例)

5/10

- Translation タブにて NAT 対象ホストを設定
 - Translated Source に inside 側ホストの NAT アドレスを新規オブジェクトにて作成し、適用

Interface Objects Translation PAT Pool Advanced

Original Packet	Translated Packet
Original Source:* in_host1 +	Translated Source: Address +
Original Destination: Address +	Translated Destination: + +
Original Source Port: + +	Translated Source Port: + +
Original Destination Port: + +	Translated Destination Port: + +

New Network Object

Name
in_mapped_host1

Description
in_host1 nat address

Network
 Host Range Network FQDN

192.168.240.200

Allow Overrides

Cancel Save

NAT 設定手順 (Manual NAT 設定例)

6/10

- Translation タブにて NAT 対象ホストを設定
 - Original Destination に outside 側ホストの実 IP アドレスで新規オブジェクトを作成し、適用

The screenshot shows the 'Translation' tab of a NAT configuration interface. It is divided into two columns: 'Original Packet' and 'Translated Packet'. The 'Original Packet' column has five rows: 'Original Source:*' (dropdown), 'Original Destination:' (dropdown with 'Address' selected and a yellow highlight), 'Original Source Port:' (dropdown), and 'Original Destination Port:' (dropdown). Each row has a '+' icon to its right. The 'Translated Packet' column has five rows: 'Translated Source:' (dropdown with 'Address' selected), 'Translated Destination:' (dropdown), 'Translated Source Port:' (dropdown), and 'Translated Destination Port:' (dropdown). Each row has a '+' icon to its right.

The screenshot shows the 'New Network Object' dialog box. It has a title bar with a question mark icon. The 'Name' field contains 'out_host1' with a yellow highlight. The 'Description' field is empty. The 'Network' section has four radio buttons: 'Host' (selected), 'Range', 'Network', and 'FQDN'. Below the radio buttons is a text field containing '192.168.240.50' with a yellow highlight. There is a checkbox for 'Allow Overrides' which is unchecked. At the bottom right, there are 'Cancel' and 'Save' buttons.

NAT 設定手順 (Manual NAT 設定例)

7/10

- Translation タブにて NAT 対象ホストを設定
 - Translated Source に inside 側ホストの NAT アドレスを新規オブジェクトにて作成し、適用

The screenshot shows the 'Translation' tab in a configuration interface. It is divided into two columns: 'Original Packet' and 'Translated Packet'. Each column has several fields with dropdown menus and plus signs for adding more items.

Original Packet	Translated Packet
Original Source:* in_host1	Translated Source: Address
Original Destination: Address	Translated Source: in_mapped_host1
Original Source Port: [empty]	Translated Destination: [empty]
Original Destination Port: [empty]	Translated Source Port: [empty]
	Translated Destination Port: [empty]

The screenshot shows the 'New Network Object' dialog box. It has a 'Name' field with the value 'out_mapped_host1', a 'Description' field with the value 'out_host1 nat address', and a 'Network' section with radio buttons for 'Host', 'Range', 'Network', and 'FQDN'. The 'Host' radio button is selected, and the 'Network' field contains the value '192.168.1.50'. There is also an 'Allow Overrides' checkbox which is unchecked. At the bottom right, there are 'Cancel' and 'Save' buttons.

NAT 設定手順 (Manual NAT 設定例)

8/10

- 必要項目の設定終了後、OK を選択し、設定を適用する (PAT Pool、Advanced タブは本前提では設定対象外)

The screenshot shows a configuration window with four tabs: "Interface Objects", "Translation", "PAT Pool", and "Advanced". The "Translation" tab is selected and highlighted. The window is divided into two columns: "Original Packet" on the left and "Translated Packet" on the right. Each column contains five rows of configuration fields, each with a plus sign to its right. The "Original Packet" fields are: "Original Source:*" (dropdown: in_host1), "Original Destination:" (dropdown: Address), "Original Source Port:" (empty dropdown), and "Original Destination Port:" (empty dropdown). The "Translated Packet" fields are: "Translated Source:" (dropdown: Address), "Translated Destination:" (dropdown: in_mapped_host1), "Translated Source Port:" (empty dropdown), and "Translated Destination Port:" (empty dropdown). At the bottom right of the window are two buttons: "Cancel" and "OK".

NAT 設定手順 (Manual NAT 設定例)

9/10

- NAT ポリシーにルールを追加後、Save ボタンで設定を保存

FTDv01_NAT_Policy
For FTDv01

You have unsaved changes [Show Warnings](#) [Save](#) [Cancel](#)

Policy Assignments (1)

Rules

[Filter by Device](#) Filter Rules [Add Rule](#)

#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Packet			Translated Packet			Options	
					Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services		
NAT Rules Before												
1		Static	Inside_Zone	Outside_Zone	in_host1	out_host1		in_mapped_host1	out_mapped_host1		Dns:false	
Auto NAT Rules												
#		Dynamic	Inside_Zone	Outside_Zone	192.168.1.0_inside_hosts			Interface			Dns:false	
NAT Rules After												

- FTD に設定を適用するため、Deploy を行う

NAT 設定手順 (Manual NAT 設定例)

10/10

- FTD show running-config 結果

```
object network in_host1
  host 192.168.1.200
object network in_mapped_host1
  host 192.168.240.200
  description in_host1 nat address
object network out_mapped_host1
  host 192.168.1.50
  description out_host1 nat address
object network out_host1
  host 192.168.240.50

nat (Inside,Outside) source static in_host1 in_mapped_host1 destination static out_host1 out_mapped_host1

> show nat detail

Manual NAT Policies (Section 1)
1 (Inside) to (Outside) source static in_host1 in_mapped_host1 destination static out_host1
out_mapped_host1
  translate_hits = 0, untranslate_hits = 0
  Source - Origin: 192.168.1.200/32, Translated: 192.168.240.200/32
  Destination - Origin: 192.168.240.50/32, Translated: 192.168.1.50/32
```

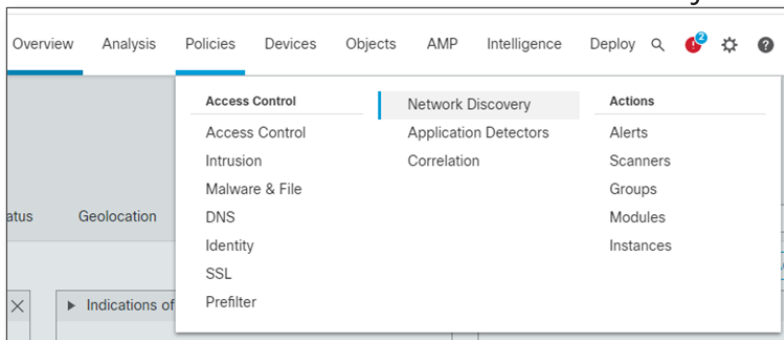
Network Discovery

Network Discovery 概要

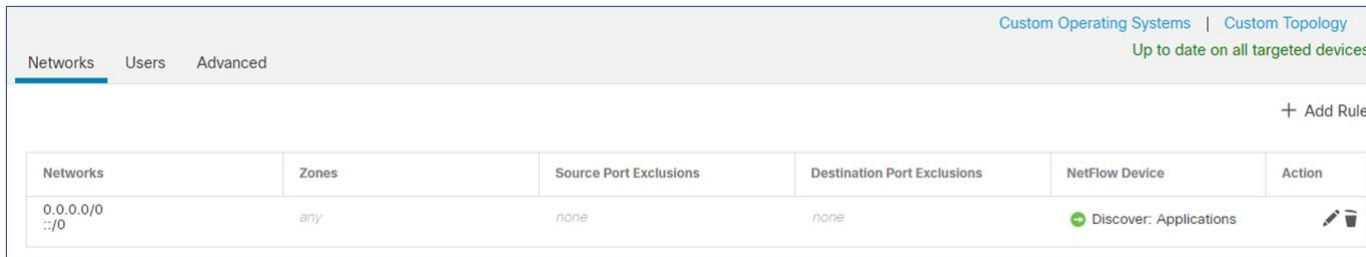
- Network Discovery 機能により FTD を通過するトラフィックに対し、ネットワーク上のホスト、アプリケーション、およびユーザーデータを収集
- 収集したデータを基に、ネットワークマップを構築し、リスクレベル、ビジネスの関連性、コンテンツカテゴリなどに基づいてアプリケーションを分類、識別する
- フォレンジック分析、プロファイリング、アクセス制御などに役立てる
- Network Discovery Policy にてホストおよびアプリケーション検出を設定する
- Network Discovery では VDB を用いアプリケーションの識別を行うため、最新の VDB への更新を推奨
- Network Discovery は FTD を通過するトラフィックに対して行われるため、ACP にて拒否されたトラフィックについては Network Discovery は機能しない
- Network Discovery は Snort Engine で処理されるため、Prefilter Fastpath を有効にしている場合は、アプリケーションの検出が行われない (Fastpath は Lina Engine (ASA 部分) でのみ動作)

Network Discovery 設定概要

- Policies > Network Discovery を選択

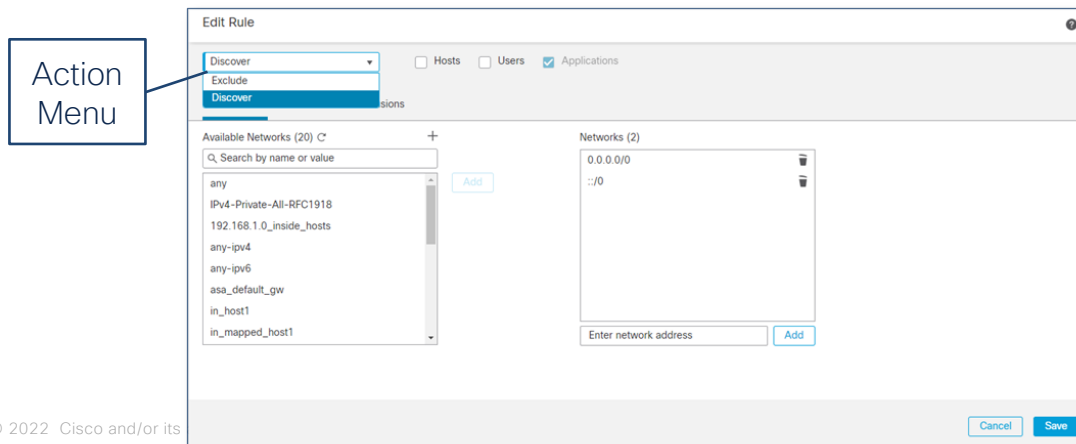
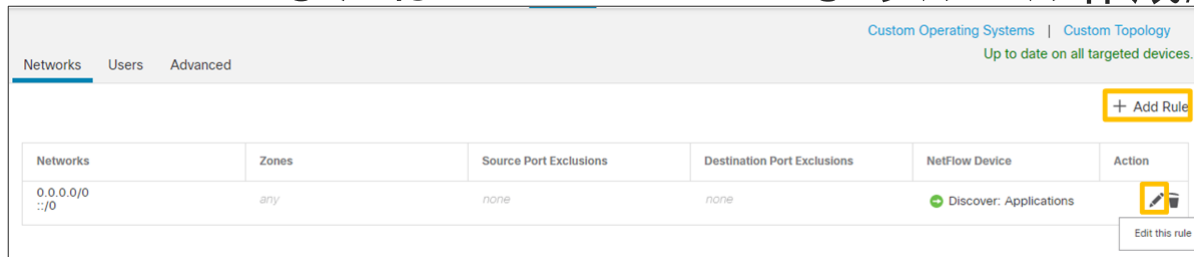


Network Discovery Policy 画面
予めデフォルトルール (全てのトラフィックに対して
アプリケーションの検知) が割り当てられている



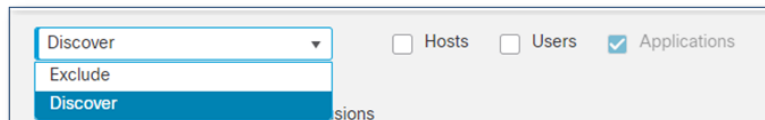
Network Discovery 設定概要

- “+ Add Rule” または “Edit this rule” よりルール作成/編集



Edit this rule を選択した際の画面。
Action には Discover、チェックボ
ックスは Applications が選択されグレイ
アウトとなっている

Network Discovery 設定概要



• Action メニュー概要

- Exclude: 監視対象から特定のネットワーク/ホストを外す際に設定。監視対象外ネットワーク / ホストから / へのトラフィックに関しては、Discovery イベントが発生しない
- Discovery / Hosts: Discovery イベントに基づいてホストをネットワークマップに追加する。(Option 設定)
- Discovery / Users: Users table にユーザを追加し、ユーザのアクティビティをユーザプロトコルのトラフィックに基づいて記録する。Users Discovery を行う場合は、Hosts Discovery の有効が必須となる。(Option 設定)
- Discovery / Applications: Application Detector に基づいてネットワークマップにアプリケーションを追加する。Applications が無効の場合、Hosts / Users の検出も行われなため、Hosts / Users 検出を行う際は Applications も必ず有効にする

Network Discovery 設定概要

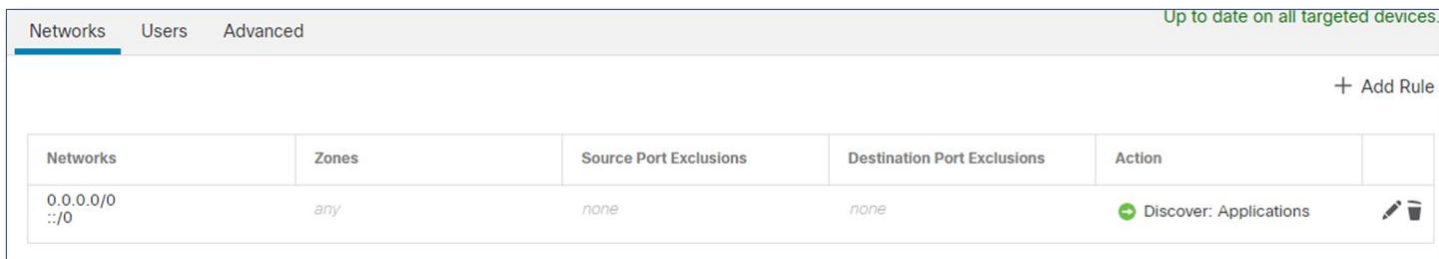
- Discovery / Hosts または Users の登録には数制限が設けられている。Hosts / Users Discovery を有効にする場合、必要な Hosts / Users セグメントにて有効にし、それぞれの Hosts / Users 制限に注意する

FMC モデル	Host Limit	User Limit
FMC1000	50,000	50,000
FMC1600	50,000	50,000
FMC2500	150,000	150,000
FMC2600	150,000	150,000
FMC4500	600,000	600,000
FMC4600	600,000	600,000
FMCv	50,000	50,000
FMCv 300	50,000	150,000



Network Discovery 設定手順

1/3

- 設定要件:
 - Application Discovery は、全てのネットワークに対して行う (Default ルールを使用)
 - Hosts / Users Discovery は Inside Network セグメントで有効にする
- 設定手順
 - Policies > Network Discovery を選択。Application Discovery においては既にデフォルトルールが設定されているため、デフォルトルールを使用。



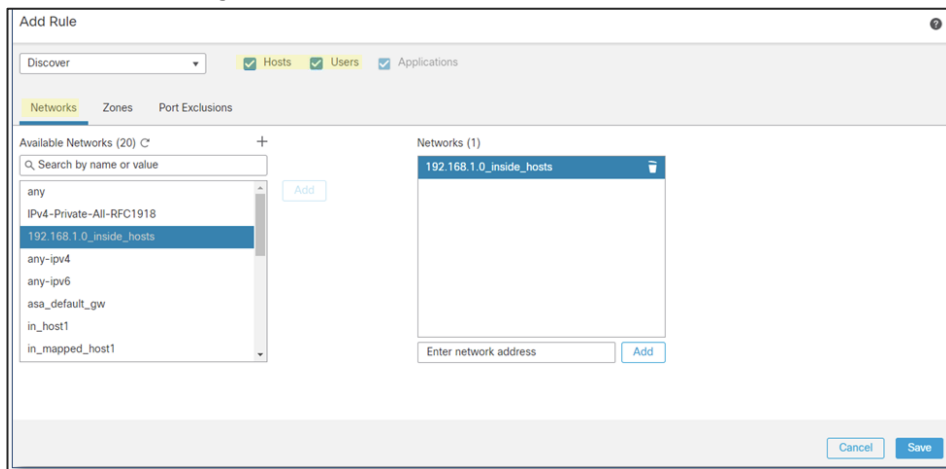
The screenshot shows the configuration page for Network Discovery. It has tabs for 'Networks', 'Users', and 'Advanced'. A status message at the top right says 'Up to date on all targeted devices.' There is a '+ Add Rule' button. Below is a table with columns: Networks, Zones, Source Port Exclusions, Destination Port Exclusions, Action, and a final column with edit/delete icons.

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

Network Discovery 設定手順

2/3

- 設定手順
 - + Add Rule にて新規ルールを追加
 - Discover アクションには Hosts / Users を選択
 - Networks > Available Networks より該当のネットワークを選択 (リストにない場合は新規 Object として作成)



Network Discovery 設定手順

3/3

- 設定手順
 - + Add Rule にて新規ルールを追加
 - Zones > Available Zones より該当のゾーンを選択
 - Save を選択し、設定を保存
 - Deploy にて設定の適用

The image shows two screenshots from a network management interface. The top screenshot is the 'Edit Rule' dialog, and the bottom screenshot is the 'Networks' table.

Edit Rule Dialog:

- Discover (dropdown)
- Hosts Users Applications
- Networks | **Zones** | Port Exclusions
- Available Zones (2) C
 - Search
 - Inside_Zone (selected) [Add]
 - Outside_Zone
- Zones (1)
 - Inside_Zone [trash]
- Buttons: Cancel, Save

Networks Table:

Networks	Zones	Source Port Exclusions	Destination Port Exclusions	Action
192.168.1.0_inside_hosts	Inside_Zone (Routed)	none	none	Discover: Hosts, Applications [edit] [trash]
0.0.0.0/0 ::/0	any	none	none	Discover: Applications [edit] [trash]

A blue arrow points from the 'Available Zones' list in the 'Edit Rule' dialog to the 'Inside_Zone' entry in the 'Networks' table.

Network Discovery 表示例

- ・トラフィックが何かしら発生した場合、Overview > Dashboard でどのようなトラフィックが来ているのか、Analysis > Hosts > Network Map にてどのホストから来ているのかなど確認できる

The screenshot shows the 'Host Profile' page in the Cisco Firepower Management Center. The host is identified as 192.168.1.101. Key details include: 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: 2022-04-07 03:29:33; Current User. Below this, there are sections for 'Indications of Compromise (0)', 'Operating Systems (2)', and 'Applications (13)'. The Operating Systems table shows a Microsoft Windows 10 system with a source of Firepower. The Applications table lists protocols like SSL and HTTPS with their respective client types.

Vendor	Product	Version	Source
Microsoft	Windows	10	Firepower

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

The screenshot shows the Network Map dashboard in the Cisco Firepower Management Center. It displays various charts and widgets. The 'Web Applications Seen' widget shows a bar chart for Microsoft HCSL with a total of 732 KB. The 'Top Client Applications Seen' widget shows a bar chart for Microsoft HCSL with a total of 5.7%. The 'Server Applications Seen' widget shows 'No Data'. The 'Top Operating Systems Seen' widget shows a bar chart for Windows with a count of 1. The dashboard also includes a search bar, a 'Reporting' button, and a 'Show the Last' dropdown set to 1 hour.

7. Prefilter の設定

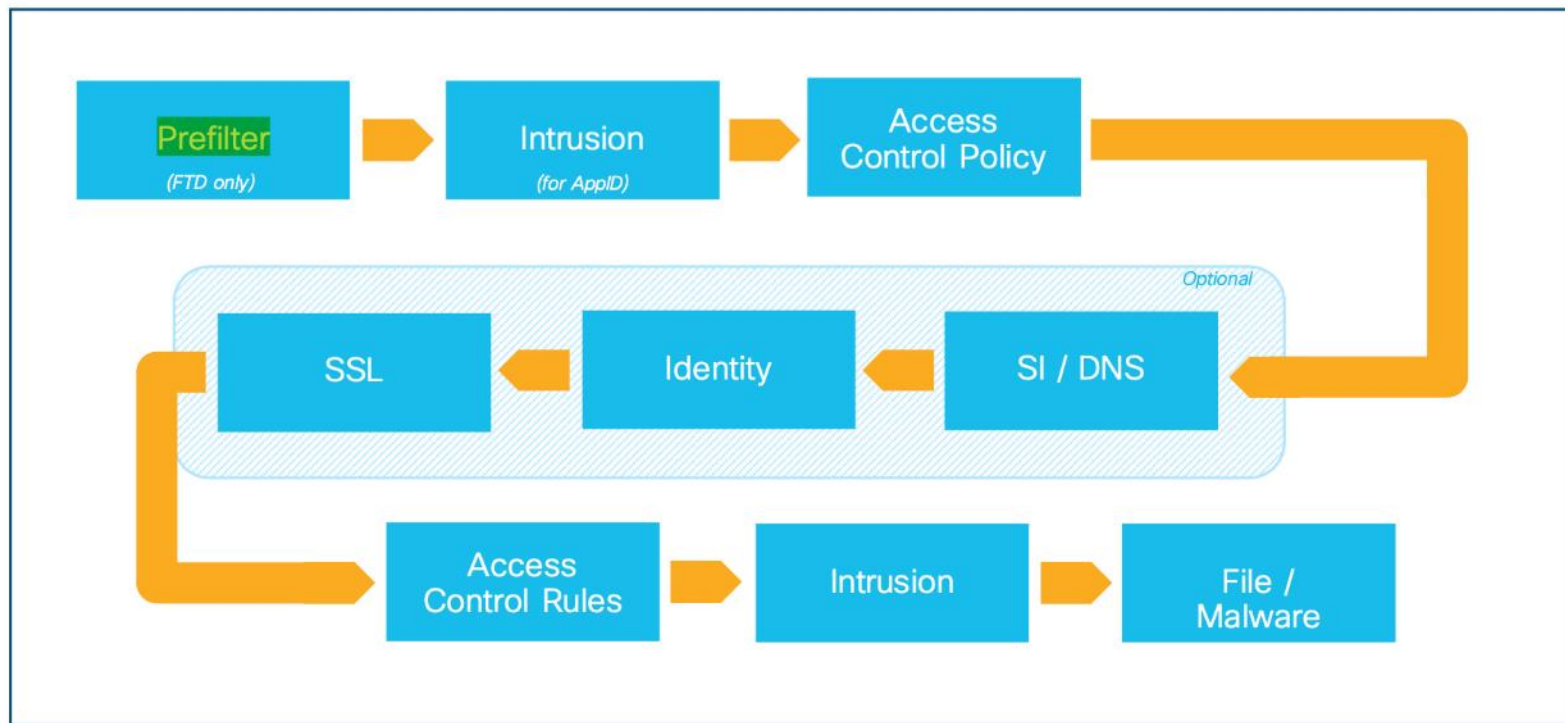
Prefilter 概要

- Access Control の中で一番最初に機能する filter である
- 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 (Snort 処理を完全にバイパス) することで回避できる

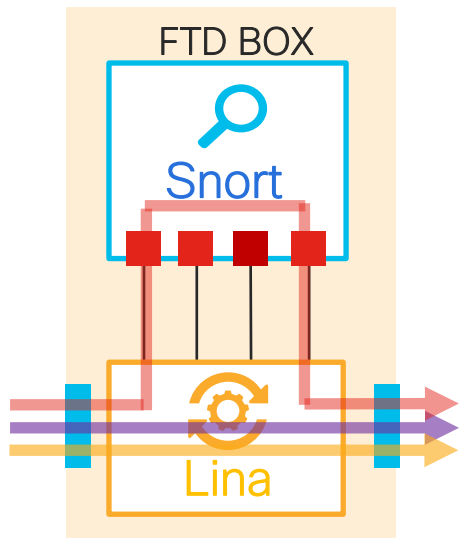
【Prefilter の利用ケース例】

- 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 エンジンを経由せずに 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 エンジンを経由せずに 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

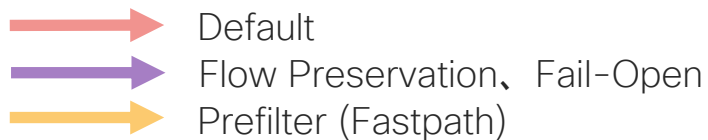
FTD 处理顺序概要



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

Characteristic	Prefiltering	Access Control
Primary function	Quickly fastpath or block certain types of plaintext, passthrough tunnels (see Encapsulation Conditions), or tailor subsequent inspection to their encapsulated traffic. Fastpath or block any other connections that benefit from early handling.	Inspect and control all network traffic, using simple or complex criteria, including contextual information and deep inspection results.
Implementation	Prefilter policy. The prefilter policy is invoked by the access control policy.	Access control policy. The access control policy is a main configuration. In addition to invoking subpolicies, access control policies have their own rules.
Sequence within access control	First. The system matches traffic to prefilter criteria before all other access control configurations.	—
Rule actions	Fewer. You can stop further inspection (Fastpath and Block) or allow further analysis with the rest of access control (Analyze).	More. Access control rules have a larger variety of actions, including monitoring, deep inspection, block with reset, and interactive blocking.
Bypass capability	Fastpath rule action. Fastpathing traffic in the prefilter stage bypasses all further inspection and handling, including: <ul style="list-style-type: none"> • Security Intelligence • authentication requirements imposed by an identity policy • SSL decryption • access control rules • deep inspection of packet payloads • discovery • rate limiting 	Trust rule action. Traffic trusted by access control rules is only exempt from deep inspection and discovery.
Rule criteria	Limited. Rules in the prefilter policy use simple network criteria: IP address, VLAN tag, port, and protocol. For tunnels, tunnel endpoint conditions specify the IP address of the routed interfaces of the network devices on either side of the tunnel.	Robust. Access control rules use network criteria, but also user, application, requested URL, and other contextual information available in packet payloads. Network conditions specify the IP address of source and destination hosts.
IP headers used (tunnel handling)	Outermost. Using outer headers allows you to handle entire plaintext, passthrough tunnels. For nonencapsulated traffic, prefiltering still uses "outer" headers—which in this case are the only headers.	Innermost possible. For a nonencrypted tunnel, access control acts on its individual encapsulated connections, not the tunnel as a whole.
Rezone encapsulated connections for further analysis	Rezones tunneled traffic. Tunnel zones allow you to tailor subsequent inspection to prefiltered, encapsulated traffic.	Uses tunnel zones. Access control uses the tunnel zones you assign during prefiltering.
Connection logging	Fastpathed and blocked traffic only. Allowed connections may still be logged by other configurations.	Any connection.
Supported devices	Firepower Threat Defense only.	All.

参考：Prefilter (Tunnel Rule) の filter について

- Prefilter (Tunnel Rule) の filter は、tunnel (GRE、IP-in-IP、IPv6-in-IP、Teredo Port 3544) traffic の外部 IP ヘッダに基づいて filtering 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 (ASA 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。

参考：Prefilter の Best Practice

【管理ネットワークトラフィック】

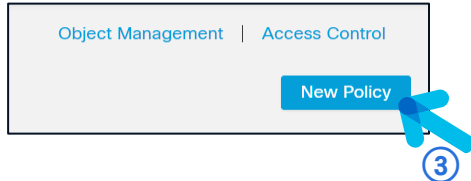
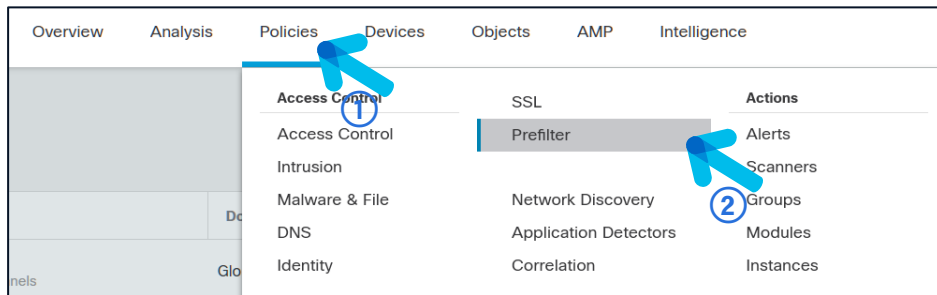
FTD を通過する管理トラフィックは fastpath する必要がある。管理トラフィックに対して（Access Control Policy を使用して）ディープインスペクションを実行すると、問題が発生する可能性があるため。

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

Prefilter (Prefilter Rule) の作成



The screenshot shows the 'New Policy' form. It has a 'Name:' field (circled with a '4') and a 'Description:' field (circled with a '5'). At the bottom, there are 'Cancel' and 'Save' buttons. Blue arrows point to the 'Name' and 'Description' fields, and another blue arrow points to the 'Save' button.

- ① Policies を選択
- ② Prefilter を選択
- ③ New Policy を選択
- ④ 任意の名前を入力
- ⑤ 必要に応じて Description を入力
- ⑥ “Save” を選択

Prefilter (Prefilter Rule) の作成

Test Prefilter Policy

Management Traffic

Analyze Hit Counts Save Cancel

Rules

+ Add Tunnel Rule + Add Prefilter Rule Search Rules X

#	Name	Rule Type	Source Interface Obj...	Destination Interface Obj...	Source Networks	Destination Networks	Source Port	Destination Port	VLAN Tag	Action	Tunnel			
There are no rules. Add Tunnel Rule Add Prefilter Rule														
Non-tunneled traffic is allowed										Default Action: Tunnel Traffic	Analyze all tunnel traffic			

① Add Prefilter Rule を選択

Prefilter (Prefilter Rule) の作成

The screenshot shows the 'Add Prefilter Rule' configuration page. The form includes the following fields and options:

- Name:** 'Test Prefilter Rule Src' (Callout 1)
- Enabled:** Checked (Callout 1)
- Action:** 'Fastpath' (Callout 1)
- Insert:** 'below rule' (Callout 1)
- Time Range:** 'None' (Callout 1)
- Interface Objects:** 'Networks' (Callout 2)
- Available Networks:** Search bar with 'in_mapped_host1' selected (Callout 3)
- Source Networks (0):** 'Add to Source' button (Callout 5)
- Destination Networks (0):** 'Add to Destination' button (Callout 5)
- Buttons:** 'Cancel' and 'Add' (Callout 6)

- 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

Prefilter (Prefilter Rule) の作成

Test Prefilter Policy You have unsaved changes [Analyze Hit Counts](#) [Save](#) [Cancel](#)

Management Traffic

[Rules](#)

+ Add Tunnel Rule + Add Prefilter Rule

#	Name	Rule Type	Source Interface Obj...	Destination Interface Obj...	Source Networks	Destination Networks	Source Port	Destination Port	VLAN Tag	Action	Tunnel Z...			
1	Test Prefilter Rule	Prefilter	any	any	inside_192.168.	any	any	any	any	Fastpath	na			0

Non-tunneled traffic is allowed Default Action: Tunnel Traffic

① Add Prefilter Rule を選択

Prefilter (Prefilter Rule) の作成

The screenshot shows the 'Add Prefilter Rule' configuration interface. It includes a header with a help icon, a descriptive paragraph about prefilter rules, and several configuration sections. The 'Name' field contains 'Test Prefilter Rule Dst' and is marked with a blue arrow and a circled '1'. The 'Enabled' checkbox is checked and also marked with a blue arrow and a circled '1'. The 'Action' dropdown is set to 'Fastpath' and is marked with a blue arrow and a circled '1'. The 'Insert' dropdown is set to 'below rule' and the 'Time Range' dropdown is set to 'None'. The 'Networks' tab is selected, and the 'Available Networks' list is visible, with 'inside_192.168.1.0' selected and marked with a blue arrow and a circled '4'. The 'Add to Destination' button is marked with a blue arrow and a circled '5'. The 'Add' button at the bottom right is marked with a blue arrow and a circled '6'.

- 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 Destination を選択
- ⑥ “Add” を選択

Prefilter (Prefilter Rule) の作成

Test Prefilter Policy

Management Traffic

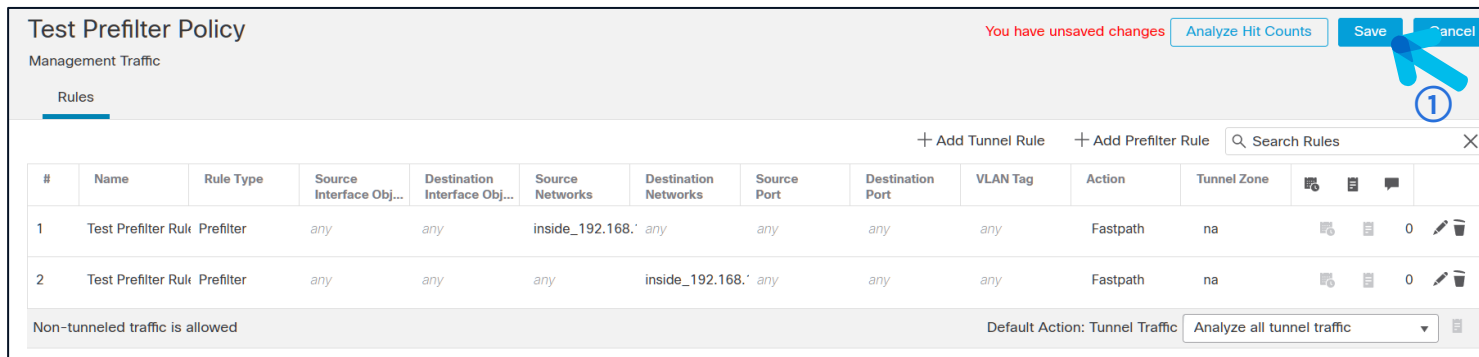
Rules

You have unsaved changes Analyze Hit Counts Save Cancel

+ Add Tunnel Rule + Add Prefilter Rule Search Rules X

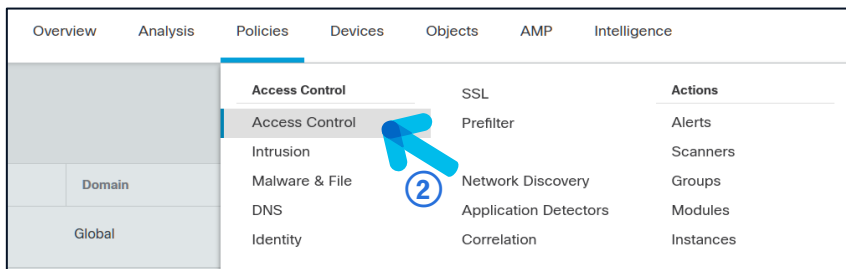
#	Name	Rule Type	Source Interface Obj...	Destination Interface Obj...	Source Networks	Destination Networks	Source Port	Destination Port	VLAN Tag	Action	Tunnel Zone			
1	Test Prefilter Rule	Prefilter	any	any	inside_192.168.	any	any	any	any	Fastpath	na			0
2	Test Prefilter Rule	Prefilter	any	any	any	inside_192.168.	any	any	any	Fastpath	na			0

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



Overview Analysis Policies Devices Objects AMP Intelligence

	Access Control	SSL	Actions
	Access Control	Prefilter	Alerts
	Intrusion		Scanners
Domain	Malware & File	Network Discovery	Groups
	DNS	Application Detectors	Modules
Global	Identity	Correlation	Instances






- ① "Save" を選択
- ② Access Control > Access Control を選択

Prefilter (Prefilter Rule) の作成

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

New Policy

Access Control Policy	Domain	Status	Last Modified	
ACP-1	Global	Targeting 1 devices <i>Up-to-date on all targeted devices</i>	2022-04-15 11:52:24 Modified by "Firepower System"	  

①

ACP-1

Enter Description

Show Warnings Analyze Hit Counts Save Cancel

Inheritance Settings | Policy Assignments (1)

Rules Security Intelligence HTTP Responses Logging **Advanced**

Prefilter Policy: **Default Prefilter Policy** SSL Policy: SSL-POLICY Identity Policy: None

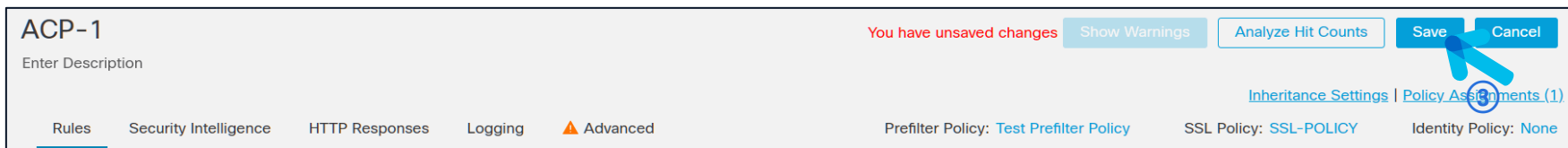
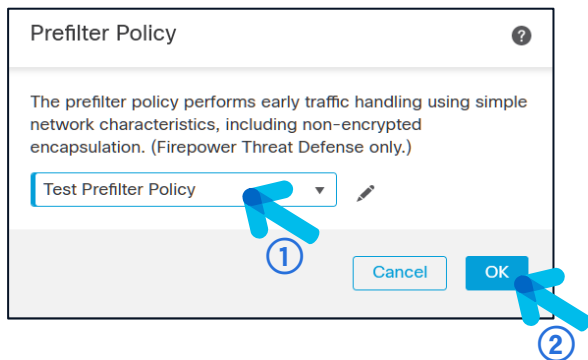
Filter by Device Search Rules X Show Rule Conflicts ? + Add Category + Add Rule

②

- ① Prefilter を適用する Access Control Policy の鉛筆マークを選択
- ② Default Prefilter Policy を選択

Prefilter (Prefilter Rule) の作成

Access Control Policy に作成した Prefilter Policy を紐づける



- ① 作成した Prefilter を選択
- ② “OK” を選択
- ③ “Save” を選択

Prefilter (Prefilter Rule) の作成

Firepower Management Center
Policies / Access Control / Policy Editor

Overview Analysis **Policies** Devices Objects AMP Intelligence

ACP-1
Enter Description

Show Warnings Analysis **Deploy** Cancel

Deployment (2)
Deployment History (3)

Inheritance Settings Policy Assignments (1)

1 device selected
Deploy time: Estimate **Deploy**

Search using device name, user name, type, group or status

Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
<input checked="" type="checkbox"/> FTD01	admin		FTD		Apr 18, 2022 1:44 PM		Pending

Access Control Group

Access Control Policy: ACP-1 admin

Prefilter Policy: Test Prefilter Policy admin

- ① “Deploy” を選択
- ② “Deployment” 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

8. Intrusion Policy 設定 (Snort3)

Snort3 概要

- Snort2 よりも効率的でパフォーマンスやスケーラビリティも向上
- FTD 7.0 以降でサポート
- FTD 単位で異なる Snort バージョンを割り当て可能

注意点：Snort3 から 2 への変更は以下の観点で非推奨

- バージョン変更の際はルールアクションは自動的に更新されないため、事前にバックアップを取って置いてダウングレード後、再設定が必要。
- Firepower recommendations は 7.0 未サポート。
 - 7.1 以降でサポートし、FMC が 7.1 以降であればその配下の FTD は 7.0.x でもサポート可能

Snort2 と Snort3 の比較

Feature	Snort2	Snort3
パケットスレッド (Packet threads)	プロセス単位で1つ (One per process)	プロセス単位で複数 (Any number per process)
メモリ消費 (Configuration memory use)	プロセス数 x GB (Number of processes* GB)	パケットに使用できるメモリが多い (GB in total: more memory available for packets)
設定リロード (Configuration reload)	遅い (Slower)	より高速。1つのスレッドを別々のコアに固定可能 (Faster:one thread can be pinned to separate cores)
構文規則 (Rule syntax)	一貫性がなく、ラインエスケープが必要 (Inconsistent and requires line escapes)	任意の空白文字で統一されたシステム (Uniform system with arbitrary whitespace)
ルールに関するコメント (Rule comments)	コメントのみ (Comments only)	#、#begin および#end マーク; C 言語スタイル (#, #begin and #end marks; C language style)

7.0 時点で非サポートの機能

Policy/Area	Features not supported
Access Control Policy	<p>The following applications settings:</p> <ul style="list-style-type: none"> • Safe Search • YouTube EDU
Threat Intelligence Detector	<p>When IPv4 or IPv6 traffic is:</p> <ul style="list-style-type: none"> • blocked: <ul style="list-style-type: none"> • No TID incident • No SI event • monitored: <ul style="list-style-type: none"> • No ITD incident

Policy/Area	Features not supported
Intrusion Policy	<ul style="list-style-type: none"> • Firepower recommendations • Policy layers • Global rule thresholding • Sensitive data detection • Logging configuration: <ul style="list-style-type: none"> • Syslog • SNMP • SRU rule updates as Snort 3 supports only LSP rule updates
Application Detection	<p>In Snort 3, by default, application detection is enabled for all networks. Unlike in Snort 2, you cannot control enabling or disabling application detection to only specific networks using network filters of the network discovery policy. For more information, see the <i>Application Detection in Snort 2 and Snort 3</i> topic in the latest version of the <i>Firepower Management Center Configuration Guide</i>.</p>
Network Discovery/RNA	<ul style="list-style-type: none"> • Host port/service identification (as seen on the network map) • OS fingerprinting (you cannot tune your intrusion policy to your network map)
Other features	Event logging with FQDN names

Intrusion Policy 概要

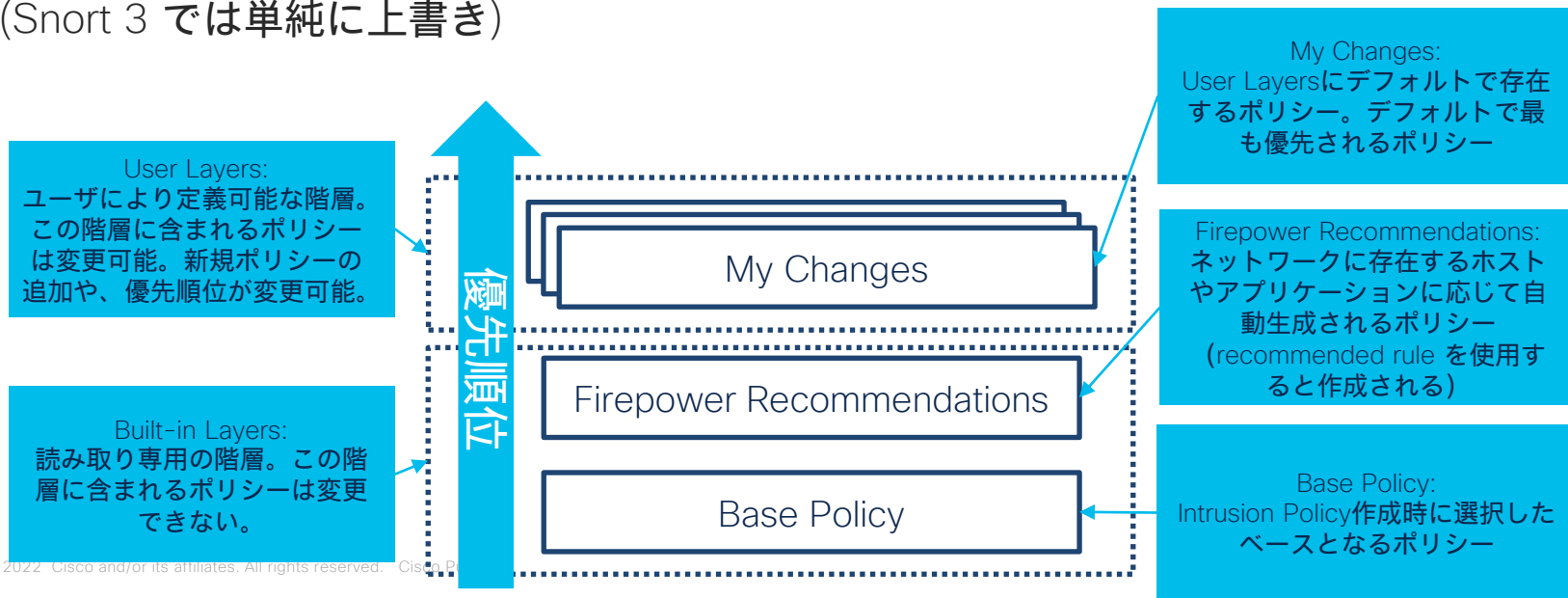
Intrusion Policy にはシグネチャに対するパラメータが含まれ、トラフィックに対する IPS の振る舞いを制御する。

■シグネチャの項目

項目	パラメータ	説明
GID:SID	—	Generator ID(GID) Snort ID(SID)
Info	—	ルールに関する情報
Rule Action	<ul style="list-style-type: none">• Block• Alert• Disable• (Revert to default)	シグネチャヒット時の動作設定 Block はブロックすると同時にイベントも作成する
Assigned Groups	—	ルールが属するカテゴリ
Comments	—	コメントの記載が可能

Intrusion Policy Snort 2 の階層ポリシー

Snort 2 での 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。(Snort 3 では単純に上書き)



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⑦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 screenshot shows the Cisco Firepower Management Center interface. The 'Policies' tab is selected, indicated by a blue arrow and a circled '1'. The breadcrumb navigation shows 'Policies > Access Control > Intrusion > Intrusion Policies', with a blue arrow and a circled '2' pointing to 'Intrusion Policies'. The 'Create Policy' button is highlighted with a blue arrow and a circled '3'. Below the navigation, there is a search bar and a table with columns: 'Intrusion Policy', 'Domain', 'Description', 'Base Policy', and 'Usage Information'. The 'Create Policy' button is also highlighted with a blue arrow and a circled '3'.

- 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 Inspection Mode を選択
- ⑥ Base Policy を選択（ベースポリシー比較ページ参照）
- ⑦ Save をクリック

The 'Create Intrusion Policy' dialog box is shown. The 'Name*' field contains 'INTRUSION_POLICY', indicated by a blue arrow and a circled '4'. The 'Description' field is empty, indicated by a blue arrow and a circled '5'. The 'Inspection Mode' section has 'Prevention' selected, indicated by a blue arrow and a circled '6'. The 'Base Policy' dropdown menu is open, showing options: 'Security Over Connectivity', 'No Rules Active', 'Maximum Detection', 'Connectivity Over Security', and 'Balanced Security and Connectivity'. The 'Balanced Security and Connectivity' option is highlighted with a blue arrow and a circled '7'. The 'Save' button is highlighted with a blue arrow and a circled '8'.

ステップ2 : POV 用にシグネチャの手動設定①


FMC
Intrusion Policies

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy 🔍 ⚙️ ⓘ Global \ admin ▾

Intrusion Policies Network Analysis Policies

Show Snort 3 Sync status ⓘ All IPS Rules **IPS Mapping ⓘ** Compare Policies Create Policy

Intrusion Policy	Domain	Description	Base Policy	Usage Information
INTRUSION_POLICY	Global	Balanced Security and...	No Access Control Policy No Device	Snort 2 Version Snort 3 Version ⓘ 📄 🗑️



① Snort 3 Version をクリック

ステップ2 : POV 用にシグネチャの手动設定②

< Intrusion Policy

Policy Name INTRUSION_POLICY

Used by: No Access Control Policy | No Device

Mode Detection | Base Policy Balanced Security and Connectivity

Disabled 36182 | Alert 467 | Block 8320 | Overridden 0

① ALL Rulesをクリック

Rule Groups

Back To Top

51 items +

Excluded | Included | Overridden

All Rules

> Browser (6 groups)

> Server (8 groups)

> Policy (1 group)

> Indicator (4 groups)

> Potentially Unwanted Applications (3 g...)

> Malware (5 groups)

> File (9 groups)

> Operating Systems (5 groups)

> Protocol (10 groups)

All Rules

All rules assigned to current intrusion policy irrespective of rule group

Rule Action

44,969 rules

Preset Filters: 467 Alert rules | 8,320 Block rules | 36,182 Disabled rules | 0 Overridden rules | [Advanced Filters](#)

<input type="checkbox"/>	GID:SID	Info	Rule Action	Assigned Groups	Comments
> <input type="checkbox"/>	1:28496 🔗	BROWSER-IE Microsoft Internet Explorer createRange u...	⚠️ Alert (Default) <input type="text"/>	Browser/Internet Explorer	🗨️
> <input type="checkbox"/>	1:32478 🔗	BROWSER-IE Microsoft Internet Explorer CSecurityCont...	⚠️ Alert (Default) <input type="text"/>	Browser/Internet Explorer	🗨️
> <input type="checkbox"/>	1:32479 🔗	BROWSER-IE Microsoft Internet Explorer CSecurityCont...	⚠️ Alert (Default) <input type="text"/>	Browser/Internet Explorer	🗨️
> <input type="checkbox"/>	1:26633 🔗	BROWSER-IE Microsoft Internet Explorer html reload loo...	⚠️ Alert (Default) <input type="text"/>	Browser/Internet Explorer	🗨️
> <input type="checkbox"/>	1:31621 🔗	BROWSER-IE Microsoft Internet Explorer onreadystatechange...	⚠️ Alert (Default) <input type="text"/>	Browser/Internet Explorer	🗨️
> <input type="checkbox"/>	1:31622 🔗	BROWSER-IE Microsoft Internet Explorer onreadystatechange...	⚠️ Alert (Default) <input type="text"/>	Browser/Internet Explorer	🗨️
> <input type="checkbox"/>	1:27766 🔗	BROWSER-PLUGINS Oracle Java Security Slider feature ...	⚠️ Alert (Default) <input type="text"/>	Browser/Plugins	🗨️

ステップ2 : POV 用にシグネチャの手動設定③

Rule Groups Back To Top

51 items +
[Excluded](#) | [Included](#) | [Overridden](#)

All Rules ①
All rules assigned to current intrusion policy irrespective of group

Rule Action ② ✕

10,259 10,259 | 44,969 rules Preset Filters: [Alert rules](#) | [Block rules](#) | [Disabled rules](#) | [Overridden rules](#) | [Advanced Filters](#)

<input checked="" type="checkbox"/>	Signature ID	Info	Rule Action	Assigned Groups	Comments
<input checked="" type="checkbox"/>	1:27144	EXPLOIT-KIT Private exploit kit outbound traffic	▲ Alert (Default) <small>(Overridden)</small>	Malware/Exploit Kit	🗨
<input checked="" type="checkbox"/>	1:25801	EXPLOIT-KIT Stamp exploit kit jar file request	▲ Alert (Default) <small>(Overridden)</small>	Malware/Exploit Kit	🗨
<input checked="" type="checkbox"/>	1:44037	INDICATOR-COMPROMISE DNS request for known mal...	▲ Alert (Default)	Indicator/Compromise	🗨
<input checked="" type="checkbox"/>	1:32005	MALWARE-BACKDOOR AlienSpy RAT outbound connec...	▲ Alert (Default)	Malware/Backdoor	🗨
<input checked="" type="checkbox"/>	1:7111	MALWARE-BACKDOOR fearless lite 1.01 runtime detecti...	▲ Alert (Default)	Malware/Backdoor	🗨
<input checked="" type="checkbox"/>	1:49517	MALWARE-CNC Unix.Trojan.Mirai variant post compromi...	▲ Alert (Default)	Malware/Command and Control	🗨
<input checked="" type="checkbox"/>	1:49514	MALWARE-CNC Unix.Trojan.Mirai variant post compromi...	▲ Alert (Default)	Malware/Command and Control	🗨
<input checked="" type="checkbox"/>	1:49794	MALWARE-CNC Unix.Trojan.Mirai variant post compromi...	▲ Alert (Default)	Malware/Command and Control	🗨
<input checked="" type="checkbox"/>	1:49791	MALWARE-CNC Unix.Trojan.Mirai variant post compromi...	▲ Alert (Default)	Malware/Command and Control	🗨

- 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④

Rule Groups Back To Top

51 items +

Excluded | Included | Overridden

All Rules

All rules assigned to current intrusion policy, irrespective of rule group

malware x

Preset Filters: Alert rules | Block rules | Disabled rules | Overridden rules | Advanced Filters

Rule Action	Assigned Groups	Comments
Alert (Default) (Overridden)	Malware/Exploit Kit	

①

Rule Action

- Block
- Alert
- Disable
- Revert to default

Save Bulk Rules

You are about to save the rule action for 10,259 rules. Do you want to continue?

Cancel Save

②

- ① "Rule Action" のプルダウンから "Block" を選択
- ② 該当するすべてのルールを変更するか聞かれるので "Save" 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 用にシグネチャの自動設定⑤

Rule Groups

51 items +

Excluded | Included | Overridden

All Rules

- > Browser (6 groups)
- > Server (8 groups)
- > Policy (1 group)
- > Indicator (4 groups)
- > Potentially Unwanted Applications (3 groups)
- ▼ Malware (5 groups)
 - Other
 - Exploit Kit

756 | 756 rules

Block

Alert

Disable

Revert to default

<input checked="" type="checkbox"/>	1:27144	EXPI
<input checked="" type="checkbox"/>	1:25801	EXPI
<input checked="" type="checkbox"/>	1:33187	EXPI
<input checked="" type="checkbox"/>	1:33186	EXPI
<input checked="" type="checkbox"/>	1:34969	EXPI
<input checked="" type="checkbox"/>	1:34970	EXPI



Save Bulk Rules

You are about to save the rule action for 756 rules. Do you want to continue?

Cancel Save

- ① Rule Groups から “exploit-kit” を選択
- 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
- ③ Rule Action プルダウンメニューを開き、Block を選択
- ④ 該当するすべてのルールを変更するか聞かれるので “Save” をクリック

ステップ2 : POV 用にシグネチャの手動設定⑥

① Rule Groups

51 items +

Excluded | Included | Overridden

All Rules

> Browser (6 groups)

> Server (8 groups)

> Policy (1 group)

Block

Alert

Disable

Revert to default

Rule Action

1:384

1 | 1 | 44,969 rules

Preset Filters: Alert rules | Block rule

GID:SIG

1:384 Info

PROTOCOL-ICMP PING



Save Bulk Rules

You are about to save the rule action for 1 rule. Do you want to continue?

Cancel

Save

- ① Rule Groups から “All Rules” を選択
- ② “1:384” をキーワードにフィルタ
- ③ チェックを入れフィルタされたシグネチャを選択
- ④ Rule Action プルダウンメニューを開き、Alert を選択
- ⑤ 該当するルールを変更するか聞かれるので “Save” をクリック

ステップ2：POV 用にシグネチャの手動設定⑦

The screenshot shows the 'Rule Groups' section of the Cisco Security Center. On the left, a sidebar lists rule groups: 'All Rules' (selected), 'Browser (6 groups)', and 'Server (8 groups)'. A blue arrow labeled '1' points to 'All Rules'. The main area shows a search bar with '1:29456' entered, and a dropdown menu for 'Rule Action' with 'Alert' selected. A blue arrow labeled '4' points to the 'Alert' option. Below the search bar, a list of rules is shown, with the first rule '1:29456' selected. A blue arrow labeled '3' points to the checkbox for this rule. A blue arrow labeled '2' points to the search bar. A blue arrow labeled '5' points to the 'Save' button in the bottom right corner of the interface.



Save Bulk Rules

You are about to save the rule action for 1 rule. Do you want to continue?

Cancel

Save

- ① Rule Groups から “All Rules” を選択
- ② “1:29456” をキーワードにフィルタ
- ③ チェックを入れフィルタされたシグネチャを選択
- ④ Rule Action プルダウンメニューを開き、Alert を選択 (第10章での試験に支障が出ることを避けるために実施)
- ⑤ 該当するルールを変更するか聞かれるので “Save” をクリック

ステップ2 : POV 用にシグネチャの手動設定⑧

Rule Groups

51 items +

Excluded | Included | Overridden

All Rules

- > Browser (6 groups)
- > Server (8 groups)
- > Policy (1 group)

Rule Action

- Block
- Alert
- Disable
- Revert to default

Search: eicar

Preset Filters: Alert rules | Block rules

8	8	44
<input checked="" type="checkbox"/>	ID:SID	
<input checked="" type="checkbox"/>	1:45909	MALWARE-CNC CobaltStrike trial version in

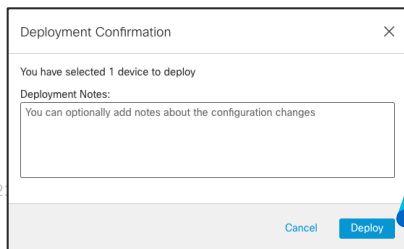
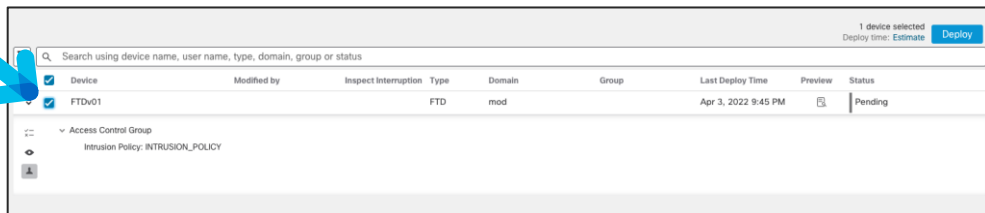
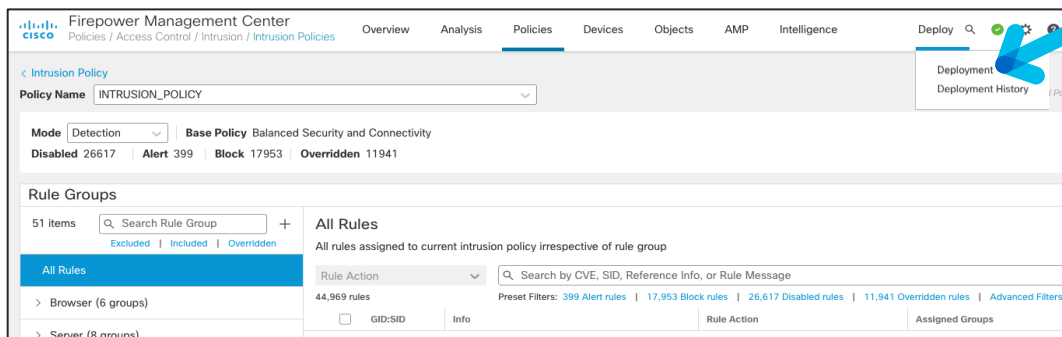
Save Bulk Rules

You are about to save the rule action for 8 rules. Do you want to continue?

Cancel Save

- 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選択
- ③ Rule Action プルダウンメニューを開き、Disable を選択
- ④ 該当するすべてのルールを変更するか聞かれるので “Save” 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

【参考情報】 Rules の検索方法 (Snort3) ①

All Rules

All rules assigned to current intrusion policy irrespective of rule group

Rule Action

44,969 rules

Preset Filters: [436 Alert rules](#) | [17,627 Block rules](#) | [26,906 Disabled rules](#) | [11,338 Overridden rules](#) | [Advanced Filters](#)



Enter GID, SID, or Reference Info to filter the rules or use any of the preset filters

Apply filter ;

Apply filter

Show

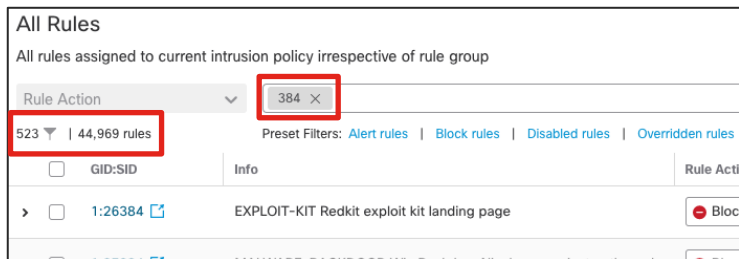
Filter by GID, SID or GID:SID ; ;

Filter by cve

Filter by comment

- Snort2 ではできなかった検索方法が可能
- Snort3 からは左記の検索オプションから実施でき、よりの絞った形の検索が可能
- ”&”条件も可能 (検索ワードを入力毎に Enter 押下)

【参考情報】 Rules の検索方法 (Snort3) ② : 検索ワード組合せ



All Rules
All rules assigned to current intrusion policy irrespective of rule group

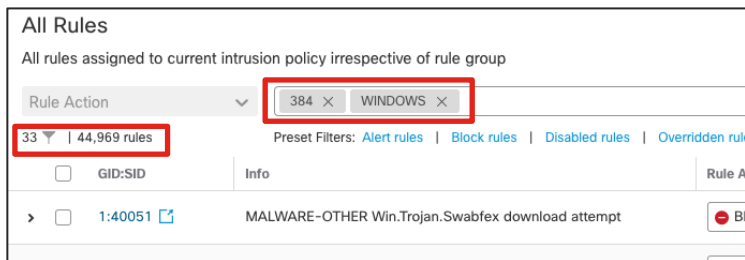
Rule Action

523 ▾ | 44,969 rules

Preset Filters: Alert rules | Block rules | Disabled rules | Overridden rules

<input type="checkbox"/>	GID:SID	Info	Rule Acti
> <input type="checkbox"/>	1:26384	EXPLOIT-KIT Redkit exploit kit landing page	Block

検索ワード "384" だけだと 523個のルールが該当



All Rules
All rules assigned to current intrusion policy irrespective of rule group

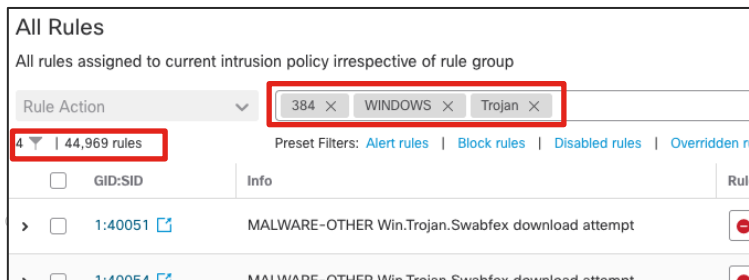
Rule Action

33 ▾ | 44,969 rules

Preset Filters: Alert rules | Block rules | Disabled rules | Overridden rule

<input type="checkbox"/>	GID:SID	Info	Rule A
> <input type="checkbox"/>	1:40051	MALWARE-OTHER Win.Trojan.Swabfex download attempt	Bl

検索ワード "384" + "WINDOWS" にすると更に 33個のルールに絞られる



All Rules
All rules assigned to current intrusion policy irrespective of rule group

Rule Action

4 ▾ | 44,969 rules

Preset Filters: Alert rules | Block rules | Disabled rules | Overridden n

<input type="checkbox"/>	GID:SID	Info	Rul
> <input type="checkbox"/>	1:40051	MALWARE-OTHER Win.Trojan.Swabfex download attempt	

更に検索ワードを追加して
"384" + "WINDOWS" + "Trojan"
にすると 4個のルールに絞られる

【参考情報】 ベースポリシーとルールセット作成のメトリック

- ・ベースポリシー（ベンダー推奨ポリシー）の選択

1. Security Over Connectivity
2. Balanced Security and Connectivity
3. Connectivity Over Security



※Maximum Detection, No Rule Activeはテスト用

- ・ルールセットを決定するためのメトリック

1. CVSS スコア
2. 脆弱性が発見されてからの経過期間
3. ルールが適用される特定の領域（影響範囲）

例) たとえば SQL インジェクションルールは、ポリシーに組み込む対象として考慮する際に、影響が十分大きい
ため重要なルールであると見なされる。

【参考情報】 ベースポリシー比較 (2022年を基準とした場合の例)

ポリシー	CVSS スコア	対象の脆弱性期間	ルールカテゴリ	説明
Maximum Detection	7.5+	2005以降	Malware-CNC, Exploit Kit	基本的にテストで使用することを目的としたポリシーでパフォーマンスにも影響。 Sid:10000以上がすべてActive(有効化)
Security over Connectivity	8+	今年+過去3年間 (2022,2021,2020, 2019)	Malware-CNC, Blacklist, SQL Injection, Exploit Kit, App-Detect	パフォーマンスよりセキュリティを優先した設定。
Balanced Security and Connectivity	9+	今年+過去2年間 (2022,2021,2020)	Malware-CNC, Blacklist, SQL Injection, Exploit Kit	デフォルトの設定。パフォーマンスとセキュリティの両方でバランスの取れた設定。
Connectivity over Security	10	今年+過去2年間 (2022,2021,2020)	-	セキュリティよりパフォーマンスを優先した設定。
No Rules Active	-	-	-	侵入検知を行わない場合(Discovery-onlyなど)に使用。初期パケットを検査せずに、すべて通過を許可する設定。

【参考情報】 例) カテゴリ単位でセキュリティレベル変更

- ステップ1で選んだ Base Policy に従ってルールグループ内のすべてのルールアクションが決定。下記の例ではステップ1で “Balanced Security and Connectivity” を選択してるため、セキュリティレベルは4段階表示の“2”になっている。 
- 例として “Browser” グループの “Firefox” に関するセキュリティレベルの変更を実施



① Browser > Firefox をクリック

② Security Level の横にある “Edit” をクリック

③ クリックすることでセキュリティレベルの変更が可能

④ Save をクリック

9. Malware & File Policy の設定

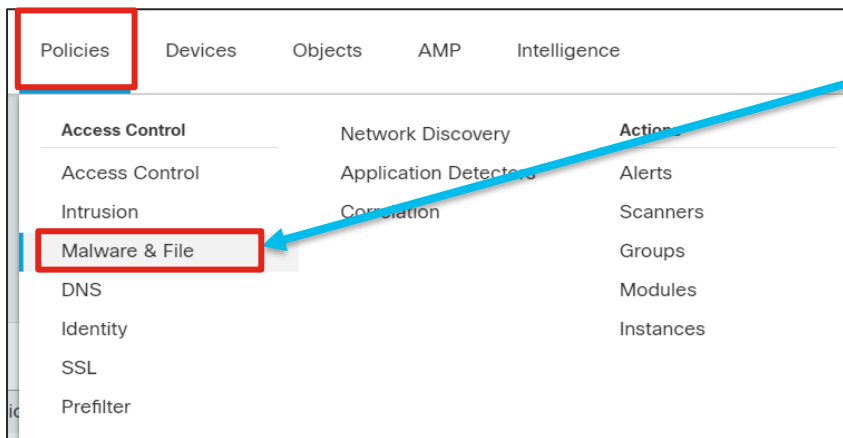
Malware & File Policy の基本事項

- Malware & File Policy では、どのトラフィック、どのファイルタイプを検査するのかを指定
- Access Control Policy で作成した Malware & File Policy を適用
 - Malware & File Policy は複数作成可能
 - 同じ Malware & File Policy を別の Access Control Policy に割り当て可能
 - Access Control Policy の Action が Allow または Interactive Block のポリシーに Malware & File Policy を適用

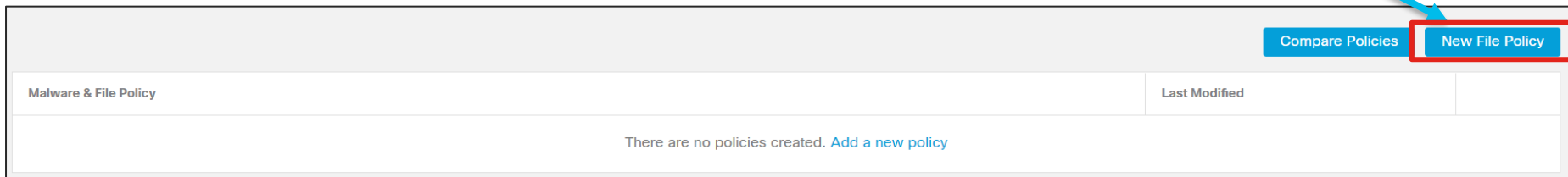
Malware & File Policy Rules

- Malware & File Policy 内のファイルカテゴリの順序は動作に影響なし
 - 1つの Malware & File Policy 内で複数のファイルルールを適用可能
- 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
 - 単純なファイルブロックはマルウェアのインスペクション/ブロックより優先
 - マルウェアインスペクション / ブロッキングは、単純な検知 / ロギングよりも優先
 - 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

File Policy の作成



1. [Policies] メニューから [Malware & File] をクリック
2. [New File Policy] をクリック



File Policy の作成-2

New File Policy



Name
File Detection Policy

Description

Cancel Save

3. [Name] 欄に任意の名前を入力（本資料では "Malware & File Policy" と命名）

4. [Save] をクリック

Malware & File Policy	Last Modified	
File Detection Policy	2022-03-16 13:52:31 Modified by "admin"	  

ルールの作成

File Detection Policy

Enter Description

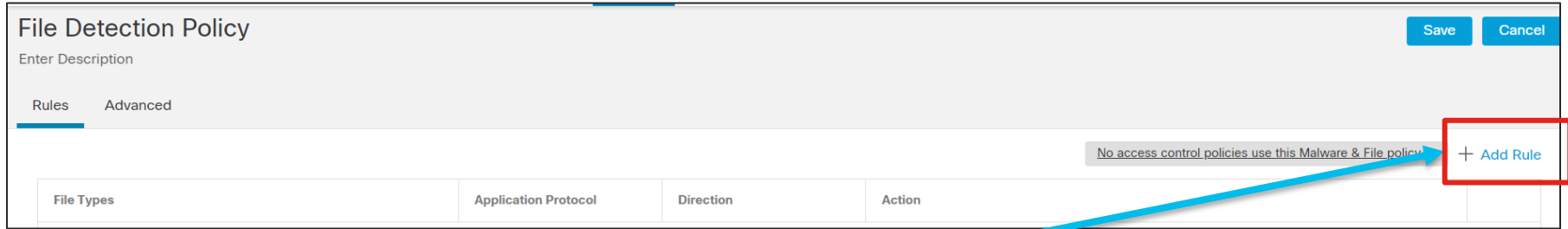
Save Cancel

Rules Advanced

No access control policies use this Malware & File policy

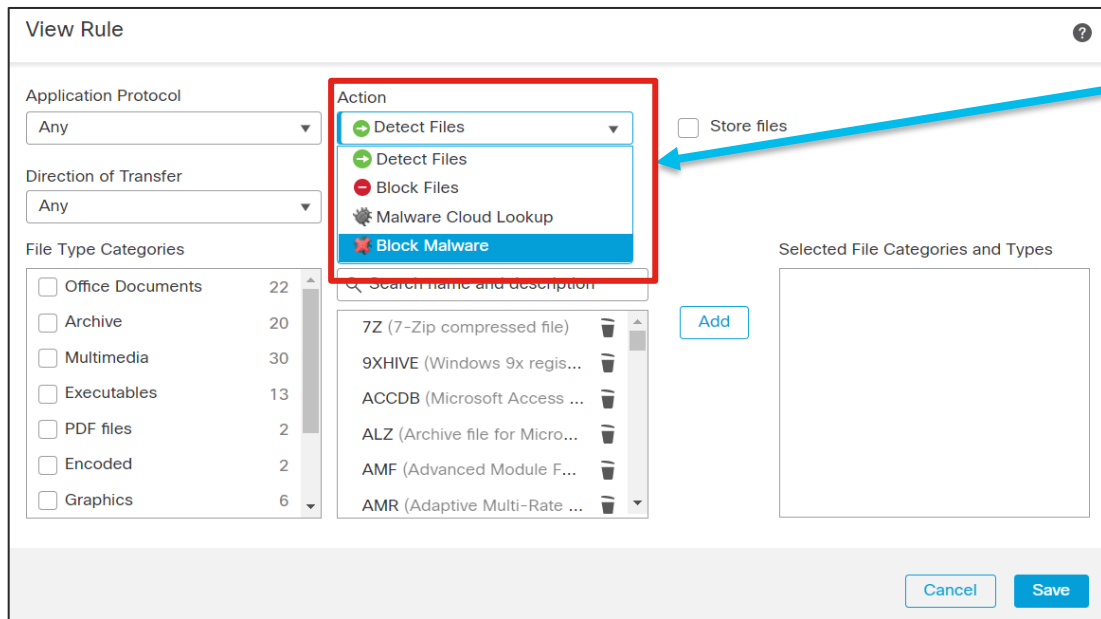
File Types	Application Protocol	Direction	Action

+ Add Rule



5. [Add Rule] をクリック

ルールの編集



6. Malware のブロックを行うため、[Action] から [Block Malware] をクリック
※その他のアクションは次ページを参照

ファイルルールアクションの種類

オプション	機能概要
Detect Files	通信は許可しログに検出の記録を実施
Block Files	指定したファイルを転送をブロックし、通信をリセット
Malware Cloud Lookup	ファイルの状態が Unknown の場合、Cloud へ状態の確認を実施、ファイルはブロックされない
Block Malware	ファイルの状態を Cloud に確認し、悪意のあるファイルの場合はファイルをブロック

ルールの編集-2

Add Rule

Application Protocol: Any

Direction of Transfer: Any

Action: Block Malware

Store Files:

- Malware
- Unknown
- Clean
- Custom

File Type Categories:

- Executables (10)
- PDF files (1)
- Encoded (0)
- Graphics (1)
- System files (4)
- Dynamic Analysis Capable (5)
- Local Malware Analysis ... (5)

File Types:

Q Search name and description

- All types in selected Category...
- 7Z (7-Zip compressed file)
- ACCDB (Microsoft Access ...)
- ALZ (Archive file for Micro...)
- ARJ (Compressed archive ...)
- BINARY_DATA (Universal ...)

Selected File Categories and Types:

- Category: Local Malware A...
- Category: Dynamic Analy...
- Category: System files
- Category: Graphics
- Category: Encoded
- Category: PDF files
- Category: Executables

Buttons: Cancel, Save

7. アクションのオプションを設定 (詳細は次ページ)
8. ファイルを保存する場合は、Store Files で任意のポジションのファイルを選択
9. 検知するファイルの種類を設定 [File Type Categories] から任意のカテゴリを選択し、[File Types] から任意のタイプを選択、すべてのタイプを選択する場合は、[All types in selected Category] をクリック
10. [Add] ボタンをクリックし、対象を追加
11. [Save] ボタンをクリックし、設定を保存

ファイルルールアクションのオプション

オプション	有効時の機能
Spero Analysis for MSEX	Unknown のファイルであれば、Windows の実行ファイルの構造を分析、クラウドに情報を送信し、マルウェアの特徴を持つファイルを検知。
Dynamic Analysis	Unknown のファイルであれば、Cisco Cloud Malware Analytics (旧 Threat Grid) にファイルを送信しサンドボックス解析を実施。
Capacity Handling	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。
Local Malware Analysis	Unknown のファイルであれば、FMC ローカルのシグネチャをベースに検査を実施。
Reset Connection	マルウェア検出時に接続をリセット (有効化推奨)。

Advanced 設定

必要に応じて Advanced タブの設定を実施

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

アーカイブファイルを検査

暗号化されたアーカイブファイルをブロック

検査できないアーカイブファイルをブロック

階層化されたアーカイブファイルの深さ（最大3階層まで）を設定

File Detection Policy

Enter Description

Rules **Advanced**

General

- First Time File Analysis
- Enable Custom Detection List
- Enable Clean List

If AMP Cloud disposition is Unknown, override disposition based upon threat score

Disabled ▾

Archive File Inspection

- Inspect Archives
- Block Encrypted Archives
- Block Uninspectable Archives

Max Archive Depth
Enter a value between 1 and 3

2

設定の配信

File Detection Policy You have unsaved changes [Save](#) [Cancel](#)

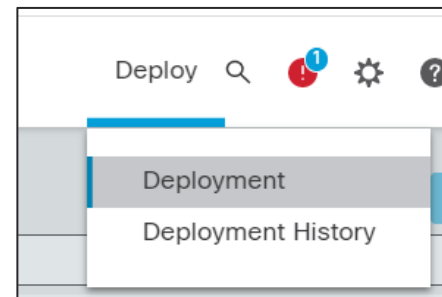
Enter Description

Rules [Advanced](#)

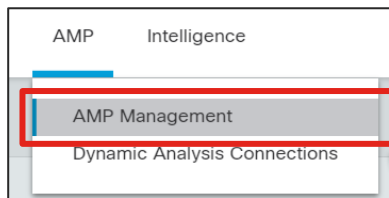
No access control policies use this Malware & File policy [+ Add Rule](#)

File Types	Application Protocol	Direction	Action
<ul style="list-style-type: none">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 AnalysisDynamic AnalysisCapacity HandlingLocal Malware AnalysisStore files of disposition: Malware

1. [Save] ボタンをクリックして設定を保存
 2. 画面右上の [Deploy] から [Deployment] をクリック
- ※本時点ではまだファイルの解析は実施されない。後述の Access Control Policy で作成したポリシーを設定する必要がある。

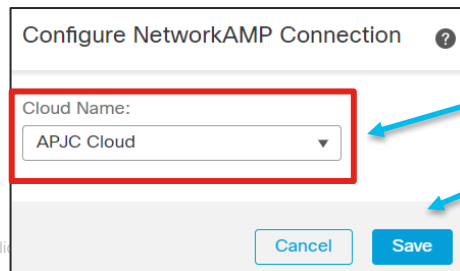
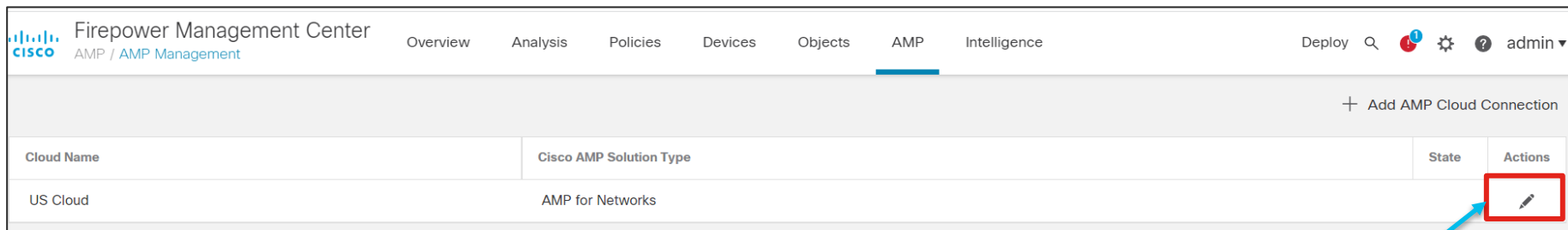


AMP 通信先の設定



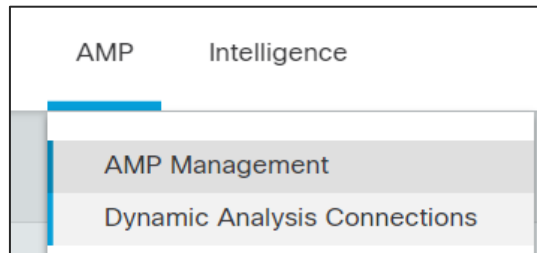
AMP Cloud はファイルハッシュのクラウドルックアップに使用される。US, EU, APJC (Asia Pacific Japan China の略) に設置されており、FMC からいちばん近い Cloud を選択することを推奨。日本に設置した FMC であれば APJC Cloud を推奨。

1. 上部メニューから [AMP] - [AMP Management] をクリック



2. [Actions] 下のペンシルマークをクリック
3. [Cloud Name] を APJC Cloud に変更し [Save] をクリック



サンドボックス解析の送信先設定



ファイルのサンドボックス解析用（Cloud Malware Analytics）の送信先の設定変更が可能。

現時点では、US または EMEA のサーバーが選択可能
※APJC のサーバーはないため設定変更しなくても可

1. 上部メニューから [AMP] - [Dynamic Analysis Connections] をクリック
2. [Actions] 下のペンシルマークをクリック
3. 送信先を設定し [Save] をクリック

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

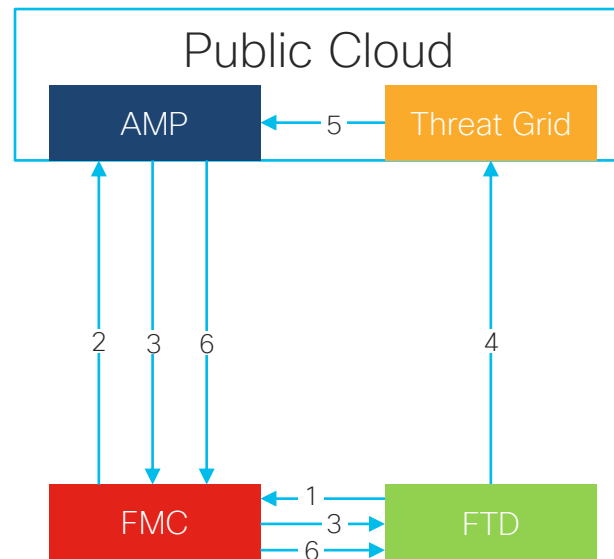
Edit Connection ?

Cloud Name:

Host:

Public クラウド環境のワークフロー

1. ファイルハッシュ (SHA) が生成され FMC にクエリを実施
2. FMC 上でディスポジションのキャッシュがない場合、FMC が AMP Cloud へ評価を確認
3. 評価の返り値:
 - Clean の場合 - ファイルは通過
 - Malware の場合 - ファイルはドロップ
 - Unknown の場合 - 事前検証用にファイルをコピーし、ファイルは通過
4. Cloud Malware Analysis (旧 Threat Grid) と連携可能な場合、ファイルは Cloud Malware Analysis で分析
5. 脅威のスコアが自動的に AMP Cloud に共有
6. AMP Cloud がディスポジションを更新し、FMC 経由で AMP の対象デバイスに共有



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



10. Access Control Policy の設定

Access Control Policy (ACP) の主なコンポーネント

- Access Control Policy はいわゆるファイアウォールポリシーに相当する。
- Intrusion Policy、Malware & File Policy、Security Intelligence とセキュリティ機能は Access Control ルールにアサインすることで動作するようになる。

L2 - L4アクセス制御

L7アクセス制御

アクション



Trust



Monitor



Allow



Block



Identity Policy

Prefilter Policy

Security Intelligence

SSL Policy

Intrusion Policy

Malware & File

URLフィルタ

作成する Access Control Policy について

1章で作成した Access Control Policy [ACP-1] へ、次のルール設定を追加する。

CATCH-ALL (IPS、Malware)

- 第7章で作成した Intrusion Policy、第8章で作成した File Policy を使用したセキュリティチェックを行う

URL-MONITOR (URL Filter、Security Intelligence)




- Security Intelligence によって配信されるネットワークおよび URL の Block List をブロックする
- URL フィルタ機能を使い、Web トラフィックの通信先 URL のカテゴリーを記録する

TIME-BASED (Time Range)

- Time Range によるアクセス制御を行う。

Access Rule の設定

- 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

Access Control Policy	Domain	Status	Last Modified	
ACP-1	Global	Targeting 1 devices <i>Up-to-date on all targeted devices</i>	2022-03-23 11:56:54 Modified by "Firepower System"	  

①

ACP-1
Enter Description

[Rules](#) [Intelligence](#) [HTTP Responses](#) [Logging](#) [Advanced](#)

[Filter by Device](#) [Search Rules](#)

[Show Warnings](#) [Analyze Hit Counts](#) [Save](#) [Cancel](#)

[Inheritance Settings](#) | [Policy Assignments \(1\)](#)

Prefilter Policy: [Default Prefilter Policy](#) SSL Policy: [None](#) Identity Policy: [None](#)

Show Rule Conflicts  [+ Add Category](#) [+ Add Rule](#)

③

- 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 [ACP-1] とし、定義右側の鉛筆マークを選択
- ② Rules タブを選択
- ③ Add Rule を選択

Access Rule の設定

Add Rule

Name: CATCH-ALL (1) Enabled Insert: into Default (3)

Action: Allow (2) Time Range: None

Zones Networks VLAN Tags Users Applications Ports URLs Dynamic Attributes **Inspection** Logging Comments

Intrusion Policy: INTRUSION_POLICY (5) Variable Set: Default Set

File Policy: File Detection Policy (6)

Snort 2 and Snort 3 version of this policy are not the same. Please make sure that any customizations are maintained independently.

- 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 として、ここでは作成済みの INTRUSION_POLICY を選択
- ⑥ 割り当てる File Policy として、ここでは作成済みの FILE Detection Policy を選択

Access Rule の設定

Add Rule

Name: CATCH-ALL Enabled Insert: into Default

Action: Allow Time Range: None

Zones Networks VLAN Tags **Users** Applications Ports URLs Dynamic Attributes Inspection **Logging** Comments

Log at Beginning of Connection **1**

Log at End of Connection **2**

File Events:

Log Files **3**

Send Connection Events to:

Firepower Management Center

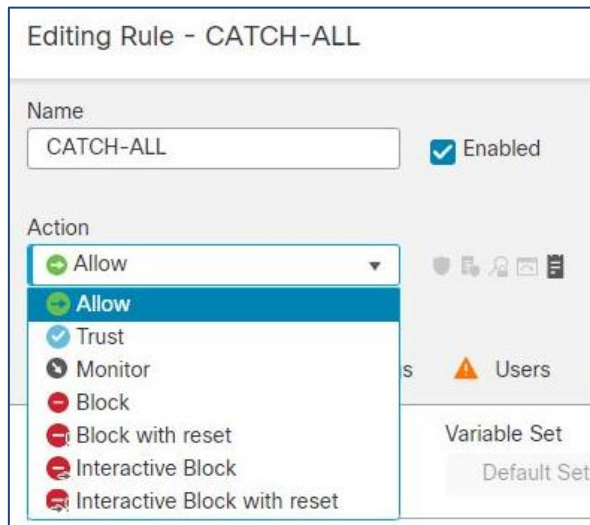
Syslog Server (Using default syslog configuration in Access Control Logging) Show Overrides

SNMP Trap Select an SNMP Alert Configurat +

Cancel **Add** **4**

- ① Logging タブを選択
- ② Log at Beginning of Connection にチェックを入れる。
なお本設定はログ取得の負荷が高い場合には不要
- ③ Log at End of Connection にチェックを入れる
- ④ Add を選択

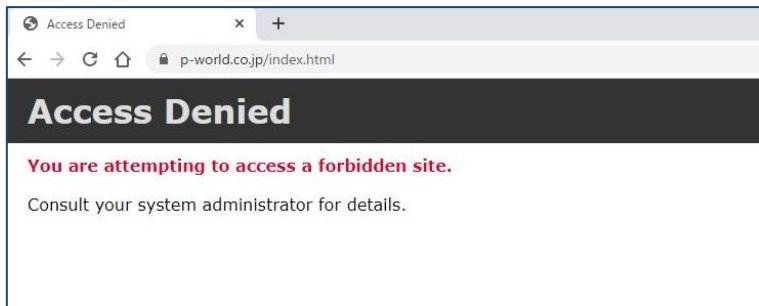
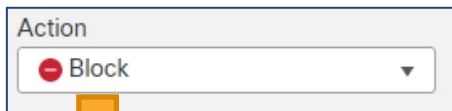
参考: Action のオプションについて



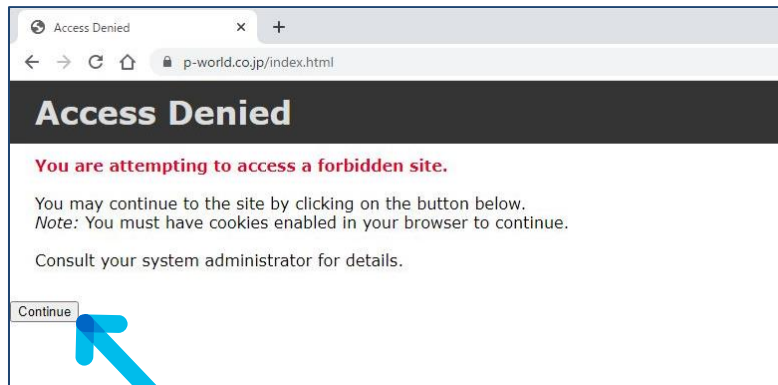
- FTD で使用できる Action は全 7 種
 - Allow: パケットを信頼せずに許可し、追加で IPS や File & Malware のチェックを実施することが可能
 - Trust: パケットを信頼して許可。IPS や File & Malware のチェックは不可
 - Monitor: ログを取るためだけに使用。トラフィックは次のルールに転送
 - Block: パケットを破棄
 - Block with reset: パケットを破棄すると同時に、送信元に対し、TCP RST パケットを送信し、通信を即遮断
 - Interactive Block: ブロックが推奨され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 with reset: 上記と同様。ただし、警告通りに通信をブロックする場合、送信元に対して TCP RST パケットを送信

参考: Action のオプションについて

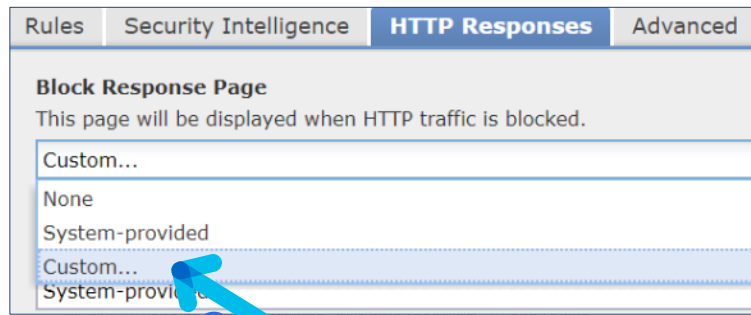
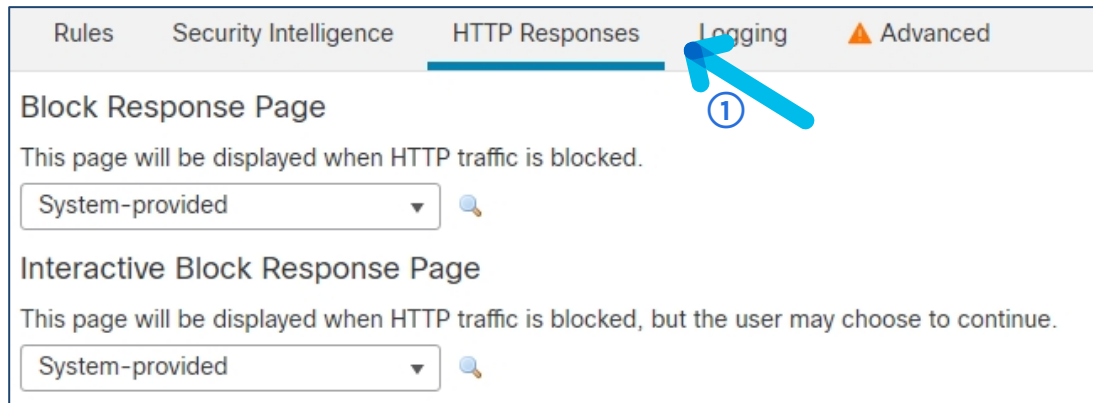
Block



Interactive Block



参考: Block 時の HTTP Response ページの編集



- ① HTTP Response ページを設定する Access Control Policy にて、HTTP Responses タブを選択
- ② 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

Edit Block Response Page

```
<!DOCTYPE html>
<html><head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<title>Access Denied</title>
<style type="text/css">body sans-serif; h1 null p null strong null</style>
</head>
<body>
<h1>Access Denied</h1>
<p>
<strong>You are attempting to access a forbidden site.</strong><br/><br/>
Consult your system administrator for details.
</p>
</body>
</html>
```

386 of 49892 characters used

デフォルト(英文)

Cancel Save

Edit Block Response Page

```
<!DOCTYPE html>
<html><head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<title>Access Denied</title>
<style type="text/css">body sans-serif; h1 null p null strong null</style>
</head>
<body>
<h1>Access Denied</h1>
<p>
<strong>閲覧の禁止されているWebサイトへのアクセスを試みようとしています。
</strong><br/><br/>
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。
</p>
</body>
</html>
```

354 of 49892 characters used

任意の日本語文に変換

Cancel Save

- ① 任意の文章に変更 (HTML 形式)
- ② Save を選択

参考: Block 時の HTTP Response ページの編集



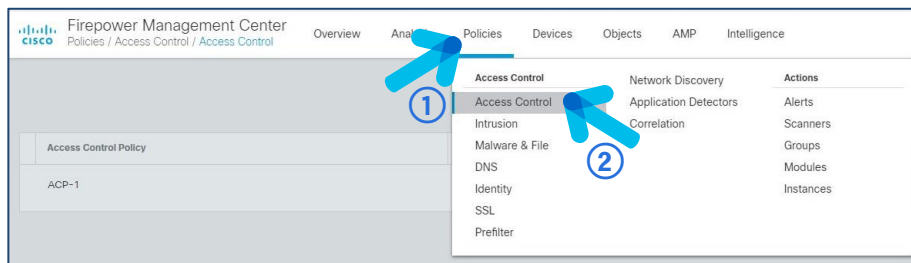
- ACP ルールにて Block される Web ページを表示させた結果、レスポンスページの表示が日本語文になっている

Security Intelligence とは

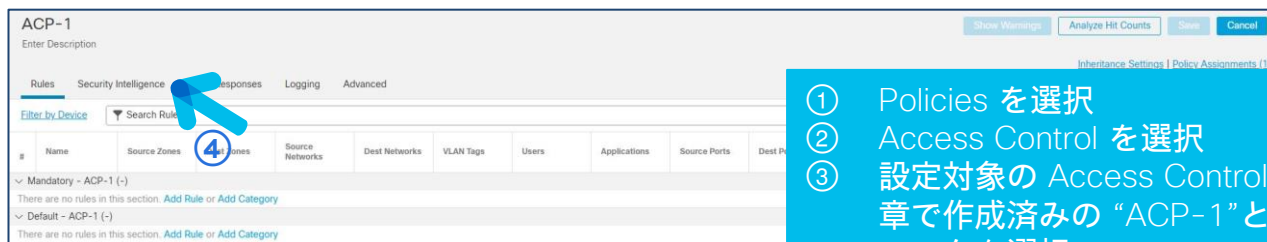
- Security Intelligence とは？
 - 一般的に言うレピュテーションに相当。例えば通信相手がマルウェアを配信する悪意のあるソースであるという「評判」がないかを分析・評価した情報。
 - Cisco Talos が随時、収集・分析したネットワークや URL のレピュテーションを提供し、ユーザは必要に応じて利用できる
 - Security Intelligence を使用する場合、FTD によるレピュテーション情報の更新頻度はデフォルトで 2 時間。設定変更の方法は「Firepower Threat Defense (FMC 管理) Version 7.0 初期セットアップガイド Vol. 1 初期インストール編」の3章「Security Intelligence ワンタイム・定期更新」を参照。

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

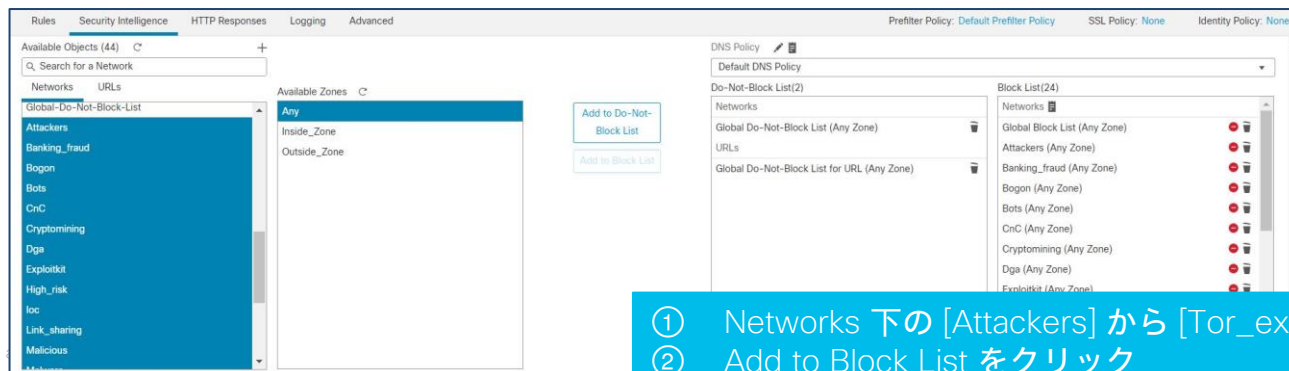
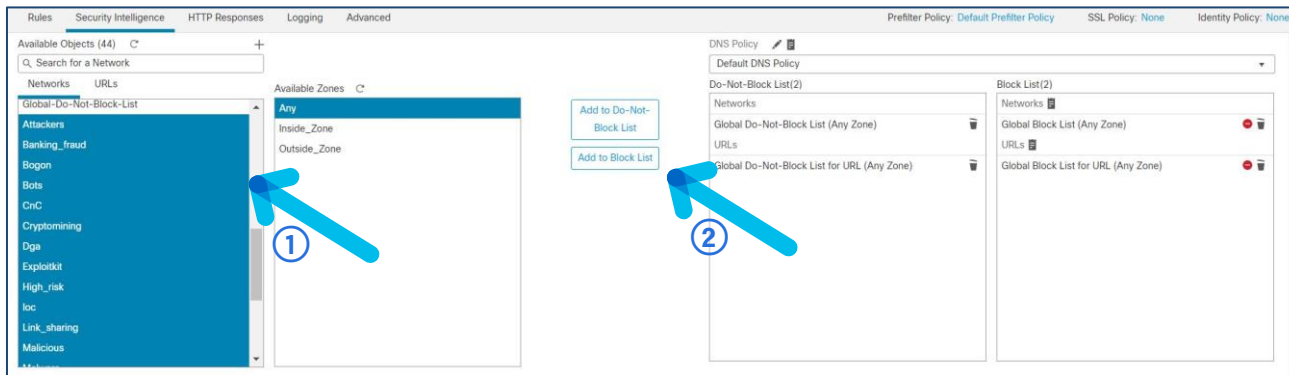


Access Control Policy	Domain	Status	Last Modified
ACP-1	Global	Targeting 1 devices Up-to-date on all targeted devices	2022-03-23 11:56:54 Modified by "Firepower System"



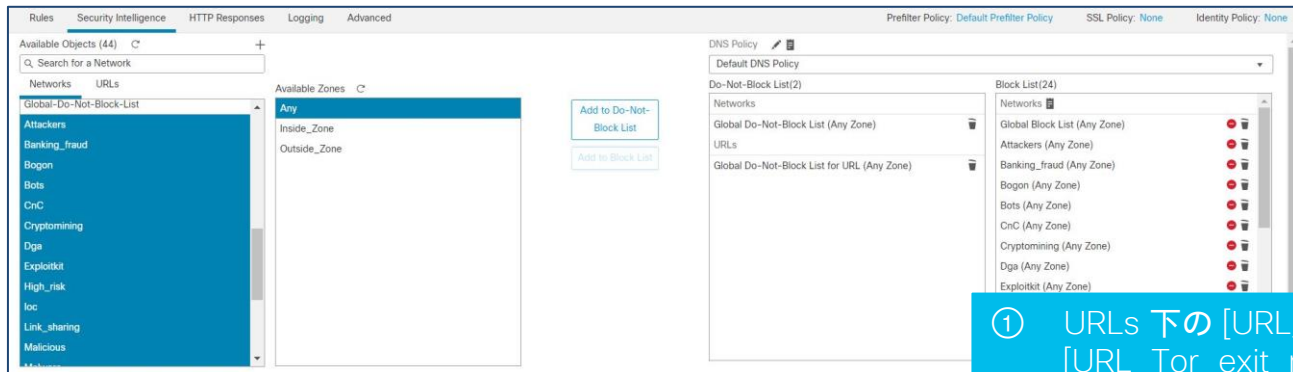
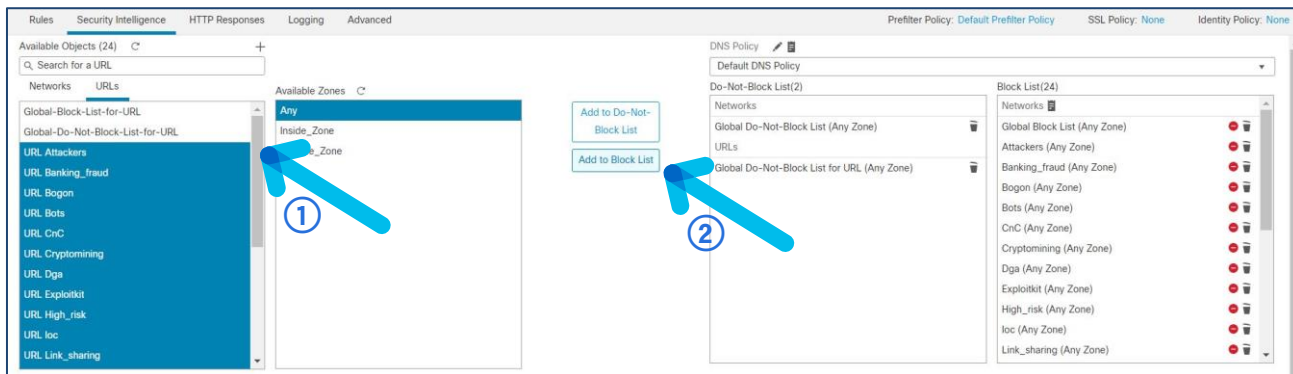
- ① Policies を選択
- ② Access Control を選択
- ③ 設定対象の Access Control Policy (ここでは1章で作成済みの“ACP-1”とする)の右側の鉛筆マークを選択
- ④ Security Intelligence を選択

Security Intelligence の設定 Network



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

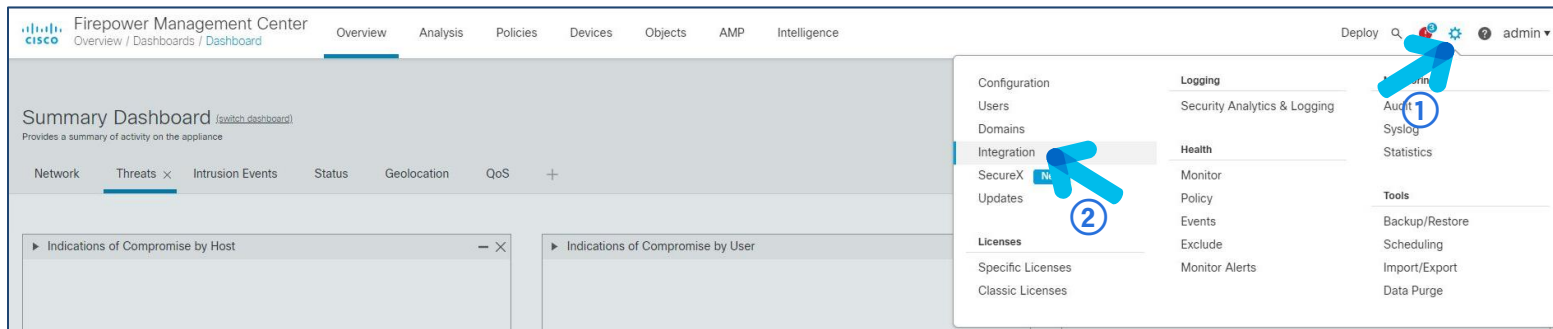
Security Intelligence の設定 URL



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

URL Filter 機能の有効化確認

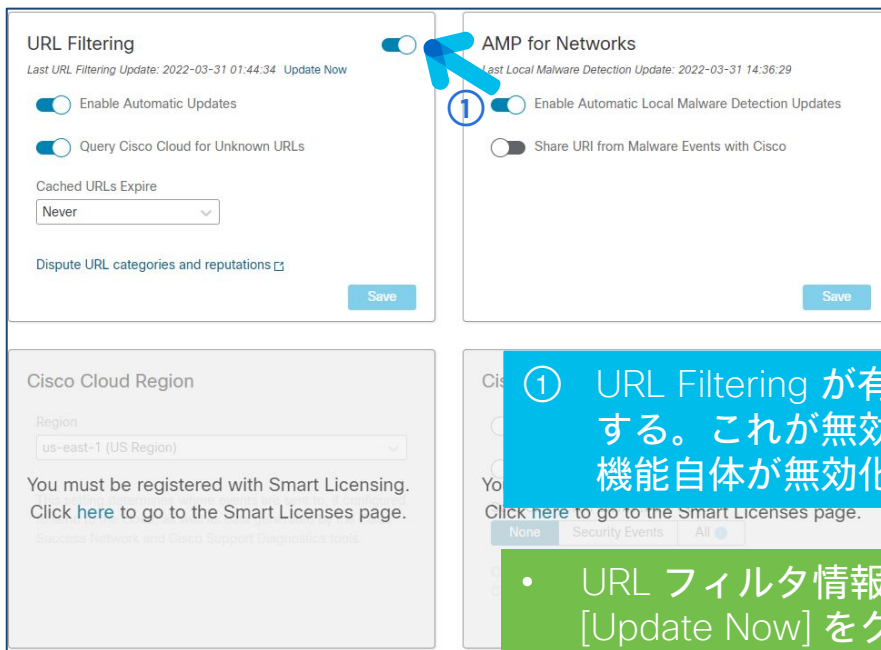
- URL Filter 機能自体が有効になっていることを確認する



- ① System を選択
- ② Integration を選択

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 configuration page for AMP for Networks. On the left, the 'URL Filtering' section has a toggle switch that is turned on (indicated by a blue arrow and a circled '1'). Below it are options for 'Enable Automatic Updates' (checked), 'Query Cisco Cloud for Unknown URLs' (checked), and 'Cached URLs Expire' (set to 'Never'). On the right, the 'AMP for Networks' section has a toggle switch for 'Enable Automatic Local Malware Detection Updates' (checked) and 'Share URI from Malware Events with Cisco' (unchecked). Both sections have 'Save' buttons at the bottom.

① 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

URL Category Monitor の設定

- 全ての通信に対し、URL カテゴリのロギングを行う Rule を追加

Access Control Policy	Domain	Status	Last Modified	
ACP-1	Global	Targeting 1 devices <i>Up-to-date on all targeted devices</i>	2022-03-23 11:56:54 Modified by "Firepower System"	

①

ACP-1
Enter Description

Show Warnings Analyze Hit Counts Save Cancel

Inheritance Settings | Policy Assignments (1)

Rules **Policy Intelligence** HTTP Responses Logging Advanced
Prefilter Policy: Default Prefilter Policy SSL Policy: None Identity Policy: None

Filter by Device Search Rules

Show Rule Conflicts + Add Category **+ Add Rule**

②

③

- 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 [ACP-1] とし、定義右側の鉛筆マークを選択
- ② Rules タブを選択
- ③ Add Rule を選択

URL Category Monitor の設定

- 全ての通信に対し、URL カテゴリのロギングを行う Rule を追加

The screenshot shows the 'Add Rule' configuration page. The 'Name' field is set to 'URL-MONITOR'. The 'Action' dropdown is set to 'Monitor'. The 'Insert' dropdown is set to 'above rule'. The 'Time Range' dropdown is set to 'None'. The 'Zones' tab is selected, showing 'Available Zones' with 'Inside_Zone' and 'Outside_Zone'. The 'Source Zones' and 'Destination Zones' sections are empty.

- 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

URL Category Monitor の設定

Editing Rule - URL-MONITOR

Name: URL-MONITOR Enabled [Move](#)

Action: Monitor Time Range: None +

Zones Networks VLAN Tags **Users** Applications Ports **URLs** Dynamic Attributes Inspection Logging Comments

Categories and URLs Search for a category

Category	URLs
Any (Except Uncategorized)	
Uncategorized	
Adult	
Advertisements	
Alcohol	

Reputations

Any
5 - Trusted
4 - Favorable
3 - Neutral
2 - Questionable
1 - Untrusted

Selected URLs (1)

Any (Except Uncategorized) (Reputations 1...)

Enter URL

- 1 URLs タブを選択
- 2 Any (Except Uncategorized) を選択
- 3 Reputations より 5 - Trusted を選択
- 4 Add to Rule をクリック
- 5 Save をクリック

- Action : Monitor の場合、Logging は Log at End of Connection が自動的に設定される

Access Control Policy 保存と Deploy

The screenshot shows the Cisco Firepower Management Center interface for editing an Access Control Policy (ACP-1). The 'Policies' tab is active. A red notification 'You have unsaved changes' is visible. The 'Save' button is highlighted with a blue arrow and a circled '1'. Other buttons include 'Analyze Hit Counts', 'Cancel', and 'Deploy'. The interface includes a search bar, a table of rules, and various configuration options like 'Inheritance Settings', 'Policy Assignments', 'Prefilter Policy', 'SSL Policy', and 'Identity Policy'.

The screenshot shows the same Cisco Firepower Management Center interface for editing ACP-1. The 'Deploy' button is highlighted with a blue arrow and a circled '2'. A dropdown menu is open over the 'Deploy' button, showing options: 'Deployment History', 'Deployment History', and 'Deployment History'. The 'Cancel' button is also visible. The interface elements are consistent with the previous screenshot.

① Save をクリック

② Deploy 下の Deployment をクリック

Access Control Policy 保存と Deploy

1 device selected
Deploy time: Estimate

Deploy

Search using device name, user name, type, group or status

Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
<input checked="" type="checkbox"/> FTDv01	admin		FTD		Mar 31, 2022 4:18 PM		Pending

Access Control Group
Access Control Policy: ACP-1

admin

Deployment Confirmation

You have selected 1 device to deploy

Deployment Notes:
You can optionally add notes about the configuration changes

Cancel Deploy

- ① >アイコンをクリックして設定変更内容を確認の上、Deploy 対象機器にチェックを入れる
- ② 画面右上の Deploy をクリック
- ③ ポップアップウィンドウにて Deploy をクリック

Access Control Policy 保存と Deploy

Firepower Management Center
Deploy / Deployment

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy 🔍 ⚙️ 👤 admin

Deploy

Search using device name, user name, type, group or status

Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
FTDv01	admin		FTD		Mar 31, 2022 4:18 PM		Completed

Access Control Group
Access Control Policy: ACP-1

Deploy 🔍 ⚙️ 👤 admin

Deployments Upgrades Health Tasks Show Notifications

20+ total 0 waiting 0 running 0 retrying 20+ success 1 failure 🔍 Filter

- Policy Deployment
Policy Deployment to FTDv01. Applied successfully 58s ×
- Policy Pre-Deployment
Pre-deploy Device Configuration for FTDv01 success 3s ×
- Policy Pre-Deployment
Pre-deploy Global Configuration Generation success 15s ×
- Policy Deployment
Policy Deployment to FTDv01. Applied successfully 1m 1s ×

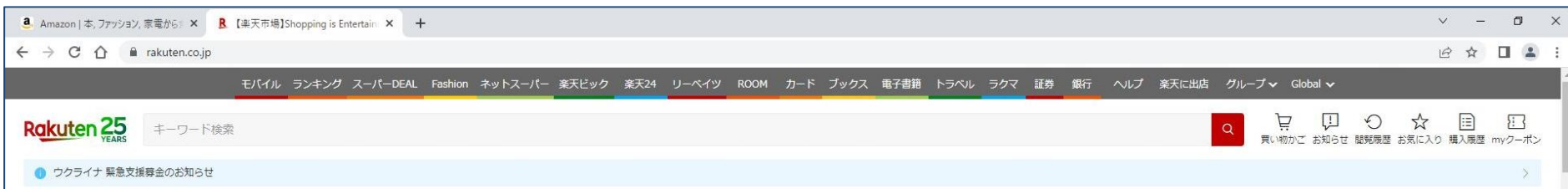
Remove completed tasks

① Status が Completed となれば Deploy の完了となる。

- Deploy ステータスは Notifications 下の Tasks でも確認が可能。画面の例では [Policy Deployment to FTDv01. Applied successfully] と表示されていることがわかる。

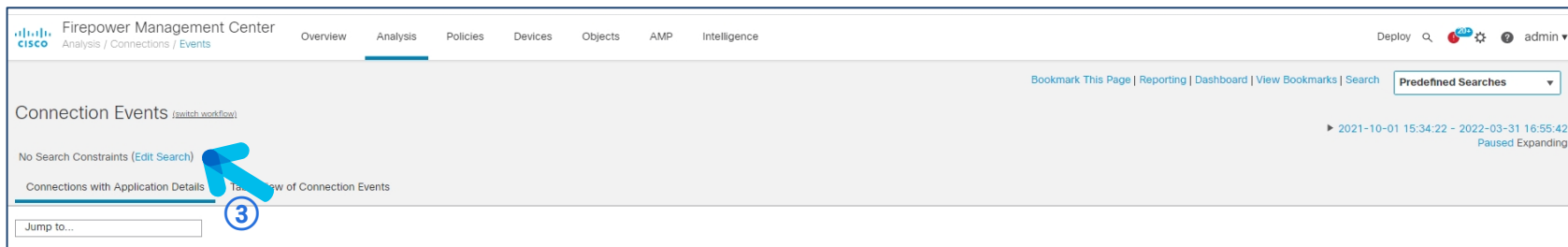
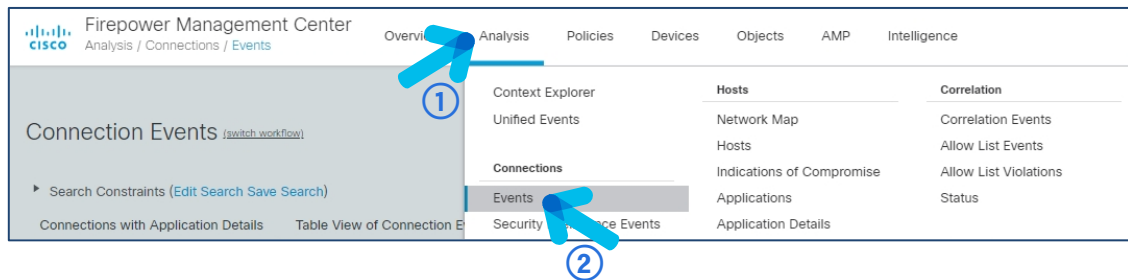
URL Filter のテスト

- 本テストでは、複数のショッピングサイトにアクセスし、URL が正しくカテゴライズされるかを確認する



① クライアント端末の Web ブラウザよりショッピングサイト (ここでは <https://www.rakuten.co.jp/>、<https://www.amazon.co.jp/>) にアクセス

URL Filter のテスト



- ① Analysis を選択
- ② Connections 下の Events を選択
- ③ Edit Search を選択

URL Filter のテスト

Connection Events

Search

(unnamed search) Private

URL

URL

URL Category

URL Reputation

Netflow

Sections

- General Information
- Networking
- Geolocation
- Device
- SSL
- Application **1**
- URL **2**

3

- ① Search より URL を選択
- ② URL のテキストボックスに、確認対象の URL を入力
- ③ Search をクリック

URL Filter のテスト

Connection Events [\[switch workflow\]](#)

▶ 2021-10-01 15:34:22 - 2022-03-31 16:55:42

Paused Expanding

▶ Search Constraints ([Edit Search](#) [Save Search](#))

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

Jump to...

<input type="checkbox"/>	↓ First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Web Application	URL	URL Category	URL Reputation	Device
▼ <input type="checkbox"/>	2022-03-31 16:55:25	2022-03-31 16:55:31	Allow		192.168.1.101		64.103.36.133		inside_zone	outside_zone	16087 / tcp	8080 / tcp	<input type="checkbox"/> HTTP	<input type="checkbox"/> Chrome	<input type="checkbox"/> Rakuten	https://www.rakuten.co.jp/	Shopping	Favorable	FTDv01
▼ <input type="checkbox"/>	2022-03-31 16:55:25		Allow		192.168.1.101		64.103.36.133		inside_zone	outside_zone	16087 / tcp	8080 / tcp	<input type="checkbox"/> HTTP	<input type="checkbox"/> Chrome	<input type="checkbox"/> Rakuten	https://www.rakuten.co.jp/	Shopping	Favorable	FTDv01

Connection Events [\[switch workflow\]](#)

▶ 2021-10-01 15:34:22 - 2022-03-31 16:55:42

Paused Expanding

▶ Search Constraints ([Edit Search](#) [Save Search](#))

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

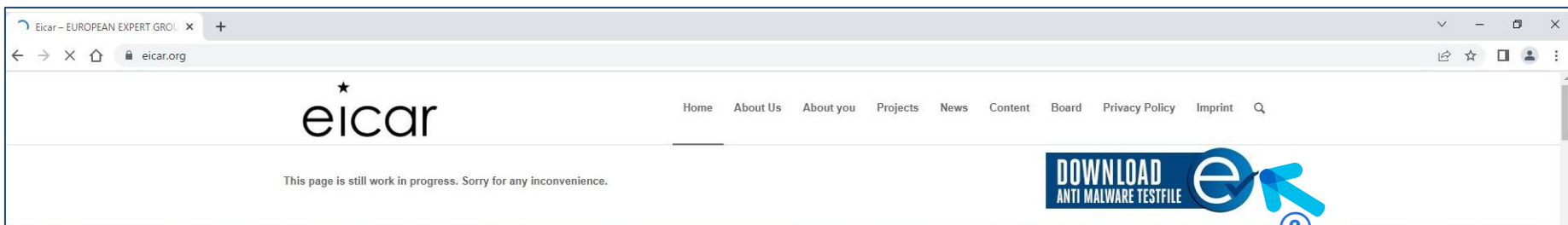
Jump to...

<input type="checkbox"/>	↓ First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Web Application	URL	URL Category	URL Reputation	Device
▼ <input type="checkbox"/>	2022-03-31 16:55:12		Allow		192.168.1.101		64.103.36.133		inside_zone	outside_zone	16031 / tcp	8080 / tcp	<input type="checkbox"/> HTTP	<input type="checkbox"/> Chrome	<input type="checkbox"/> Amazon	https://www.amazon.co.jp/	Shopping	Favorable	FTDv01

① URL カテゴリで Shopping と分類されていることを確認する

AMP (File Policy) のテスト

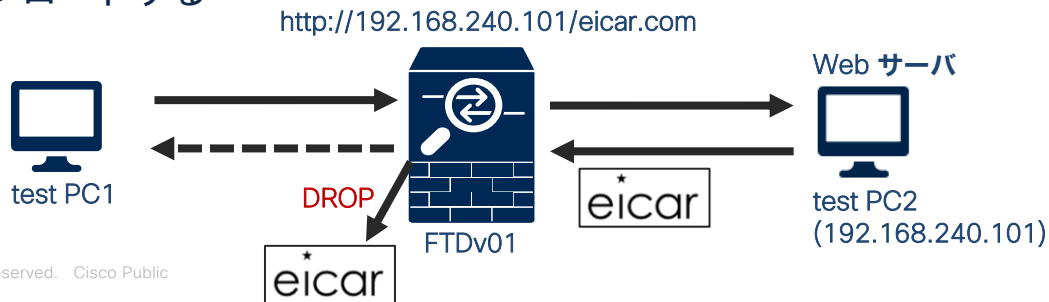
- 本テストでは、テスト用のマルウェアファイルをクライアント端末にダウンロードし、AMP Policy がマルウェアを正しく検知できるかを確認する



- ① クライアント端末の Webブラウザより <https://www.eicar.org/> にアクセス
- ② DOWNLOAD ANTI MALWARE TESTFILE をクリック

AMP (File Policy) のテスト

- 本テストでは、テスト用のマルウェアファイル (eicar.com) 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
- eicar.com のファイルは <https://www.eicar.org> より事前に入手し、test PC2 に配備しておく。test PC2 は http サーバとして動作させ、test PC1 から eicar.com をダウンロードを実施するも失敗することで本テストの実施とする (これらの準備、設定、実施は本資料では割愛)
- https での通信のセキュリティインスペクションを行うには、Vol.3 の TLS decryption の設定が必要であり、本章ではテスト簡素化のために TLS decryption 実施前の状態でテスト用のマルウェアファイルをダウンロードする



AMP (File Policy) のテスト

The screenshot shows the Firepower Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. A blue arrow labeled '1' points to the 'Analysis' tab. The main content area is titled 'Malware Summary' and includes a search bar and a table of detection names. A blue arrow labeled '2' points to the 'Malware Events' link in the left-hand navigation menu under the 'Files' section.

- ① Analysis を選択
- ② Files 下の Malware Events を選択

AMP (File Policy) のテスト

Malware Summary (switch workflow) || 2022-04-25 15:11:14 - 2022-04-25 16:13:26
Expanding

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

Malware Summary **Table View of Malware Events**

Jump to...

<input type="checkbox"/>	Detection Name	File Name	File SHA256	File Type	↓ Count
▼ <input type="checkbox"/>	EICAR	/eicar.com	🔴 275a021b...f651fd0f	EICAR	1

⏪ < Page 1 of many > ⏩ Displaying row 1 of many rows

[View](#) [Delete](#)
[View All](#) [Delete All](#)

- ① EICAR によるマルウェアイベントが検出されていることを確認する
- ② 送信元・先 IP アドレス、検出時刻を確認するため、Table View of Malware Events をクリック

AMP (File Policy) のテスト

Malware Summary [\(switch workflow\)](#)

|| 2022-04-25 15:11:14 - 2022-04-25 16:18:36
Expanding

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

Malware Summary Table View of Malware Events

Jump to...

	<input type="checkbox"/>	↓ Time ×	Action ×	Sending IP ×	Sending Country ×	Receiving IP ×	Receiving Country ×	Sending Port ×	Receiving Port ×	SSL Status ×	User ×	Event Type ×	Event Subtype ×	Detection Name ×	File Name ×	File SHA256 ×	Threat Score ×	File Pa
▼	<input type="checkbox"/>	2022-04-25 16:18:26	Malware Block	192.168.240.101		192.168.1.101		80 (http) / tcp	51711 / tcp			Threat Detected in Network File Transfer		EICAR	eicar.com	275a021b...f651fd0f	●●●● Very High	
▼	<input type="checkbox"/>	2022-04-25 16:18:24	Malware Block	192.168.240.101		192.168.1.101		80 (http) / tcp	51710 / tcp			Threat Detected in Network File Transfer		EICAR	eicar.com	275a021b...f651fd0f	●●●● Very High	
▼	<input type="checkbox"/>	2022-04-25 16:18:22	Malware Block	192.168.240.101		192.168.1.101		80 (http) / tcp	51709 / tcp			Threat Detected in Network File Transfer		EICAR	eicar.com	275a021b...f651fd0f	●●●● Very High	
▼	<input type="checkbox"/>	2022-04-25 16:18:20	Malware Block	192.168.240.101		192.168.1.101		80 (http) / tcp	51708 / tcp			Threat Detected in Network File Transfer		EICAR	eicar.com	275a021b...f651fd0f	●●●● Very High	
▼	<input type="checkbox"/>	2022-04-25 16:18:00	Malware Block	192.168.240.101		192.168.1.101		80 (http) / tcp	51707 / tcp			Threat Detected in Network File Transfer		EICAR	eicar.com	275a021b...f651fd0f	●●●● Very High	
▼	<input type="checkbox"/>	2022-04-25 16:17:59	Malware Block	192.168.240.101		192.168.1.101		80 (http) / tcp	51706 / tcp			Threat Detected in Network File Transfer		EICAR	eicar.com	275a021b...f651fd0f	●●●● Very High	
▼	<input type="checkbox"/>	2022-04-25 16:17:57	Malware Block	192.168.240.101		192.168.1.101		80 (http) / tcp	51705 / tcp			Threat Detected in Network File Transfer		EICAR	eicar.com	275a021b...f651fd0f	●●●● Very High	
▼	<input type="checkbox"/>	2022-04-25 16:17:55	Malware Block	192.168.240.101		192.168.1.101		80 (http) / tcp	51704 / tcp			Threat Detected in Network File Transfer		EICAR	eicar.com	275a021b...f651fd0f	●●●● Very High	

- ① 送信元・先 IP アドレス、検出時刻などを確認する
- ② マルウェアの拡散状況を確認するため、File SHA256 の赤いアイコンをクリック

AMP (File Policy) のテスト

Network File Trajectory for 275a021b...f651fd0f

File SHA256 275a021b...f651fd0f

File Names /eicar.com , eicar.com

File Size (KB) 0.066

File Type EICAR

File Category Executables

Current Disposition Malware

Threat Score Very High

Detection Name EICAR

First Seen 2022-04-25 16:12:20 on 192.168.240.101

Last Seen 2022-04-25 16:18:26 on 192.168.240.101

Event Count 12

Seen On 1 hosts

Seen On Breakdown 1 sender → 0 receivers

Trajectory

Apr 25

16:12 16:16 16:17 16:18

192.168.240.101

Events Transfer Block Create Move Execute Scan Retrospective Quarantine

Dispositions Unknown Malware Clean Custom Unavailable

Events

Time	Event Type	Sending IP	Receiving IP	User	File Name	Disposition	Action	Protocol	Client	Web Application	De...
2022-04-25 16:12:20	Transfer	192.168.240.101	192.168.1.101		/eicar.com	Malware	Malware Block	HTTP	Firefox	Web Brow...	
2022-04-25 16:16:15	Transfer	192.168.240.101	192.168.1.101		eicar.com	Malware	Malware Block	HTTP	Firefox		
2022-04-25 16:16:30	Transfer	192.168.240.101	192.168.1.101		eicar.com	Malware	Malware Block	HTTP	Firefox		
2022-04-25 16:16:33	Transfer	192.168.240.101	192.168.1.101		eicar.com	Malware	Malware Block	HTTP	Firefox		
2022-04-25 16:17:55	Transfer	192.168.240.101	192.168.1.101		eicar.com	Malware	Malware Block	HTTP	Firefox		
2022-04-25 16:17:57	Transfer	192.168.240.101	192.168.1.101		eicar.com	Malware	Malware Block	HTTP	Firefox		

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 となっていることを確認

IPS (Intrusion Policy) のテスト

- 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 からの応答: バイト数 =32 時間 =3ms TTL=50
8.8.8.8 からの応答: バイト数 =32 時間 =3ms TTL=50
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 クライアント端末でコマンドプロンプトを起動し、ping コマンドを実行。宛先は FTD デバイスを經由した先の IP アドレスを使用すること。
- ② Ping が終了することを確認する。

- 作成済みの Intrusion Policy の Mode が Detection となっているため、パケットは破棄されずに ping コマンドによる疎通自体は可能。

IPS (Intrusion Policy) のテスト

The screenshot shows the Cisco Firepower Management Center interface. The main navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. A blue arrow labeled '1' points to the 'Analysis' tab. The left sidebar contains a search bar and a list of event categories: 'Context Explorer', 'Unified Events', 'Connections', 'Events', 'Security Intelligence Events', 'Intrusions', 'Events', 'Reviewed Events', 'Clipboard', 'Incidents', 'Files', 'Malware Events', 'File Events', 'Captured Files', and 'Network File Trajectory'. A blue arrow labeled '2' points to the 'Events' item under the 'Intrusions' category. The main content area displays 'Events By Priority and Classification' with a table view showing two rows of events: 'PROTOCOL-ICMP Unusual PING detected (1:29456:3)' and 'PROTOCOL-ICMP PING (1:384:8)'. The bottom of the interface shows pagination information: 'Page 1 of 1' and 'Displaying rows 1-2 of 2 rows'.

- ① Analysis を選択
- ② Intrusions 下の Events を選択

IPS (Intrusion Policy) のテスト

Events By Priority and Classification [switch work flow]

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

2022-04-01 17:00:00 - 2022-04-01 17:11:03
Expanding

Drilldown of Event, Priority, and Classification | Table View of Events | Packets

Jump to...

<input type="checkbox"/>	Message	↓ Priority	Classification	Count
▼ <input type="checkbox"/>	PROTOCOL-ICMP Unusual PING detected (1:29456:3)	medium	Information Leak	1
▼ <input type="checkbox"/>	PROTOCOL-ICMP PING (1:384:8)	low	Misc Activity	1

1

2

< Page 1 of 1 > | Displaying rows 1-2 of 2 rows

View Copy Delete Review Download Packets

View All Copy All Delete All Review All Download All Packets

- ① PROTOCOL-ICMP PING (1:384:8)、により攻撃が検出されていることを確認
※本環境では Intrusion Policy の設定により、[PROTOCOL-ICMP Unusual PING detected (1:29456:3)] も検知される。
- ② 送信元・先 IP アドレス、検出時刻を確認するため、Table View of Eventsをクリック

IPS (Intrusion Policy) のテスト

Events By Priority and Classification [\[switch workflow\]](#) || 2022-04-

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

Drilldown of Event, Priority, and Classification Table View of Events Packets

Jump to...

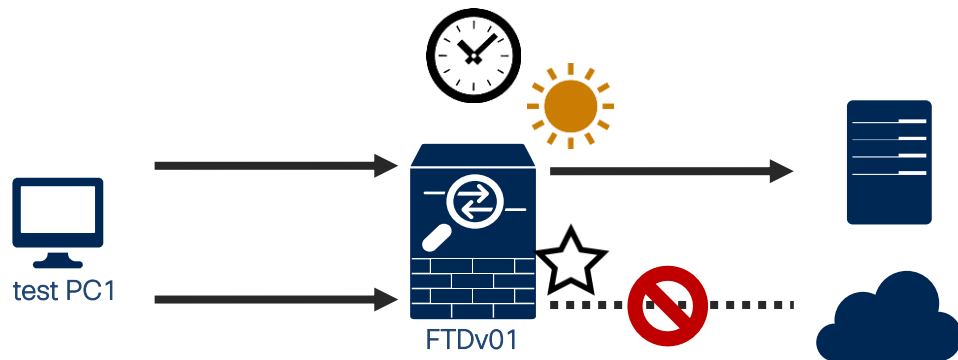
<input type="checkbox"/>	Time x	Priority x	Impact x	Inline Result x	Reason x	Source IP x	Source Country x	Destination IP x	Destination Country x	Source Port / ICMP Type x	Destination Port / ICMP Code x	SSL Status x	VLAN ID x	Message x
▼ <input type="checkbox"/>	2022-04-01 17:10:39	medium	2	⚠ Would have dropped	Intrusion Policy in "Detection" Inspection Mode	192.168.1.101		8.8.8.8	USA	8 (Echo Request) / icmp	0 (No Code) / icmp	Unknown (Unknown)	0	PROTOCOL-ICMP Unusual PING detected (1.29456:3)
▼ <input type="checkbox"/>	2022-04-01 17:10:39	low	2	⚠ Would have dropped	Intrusion Policy in "Detection" Inspection Mode	192.168.1.101		8.8.8.8	USA	8 (Echo Request) / icmp	0 (No Code) / icmp	Unknown (Unknown)	0	PROTOCOL-ICMP PING (1.384:8)

⏪ < Page of 1 > ⏩ Displaying rows 1-2 of 2 rows

① 送信元・先 IP アドレス、検出時刻などを確認する

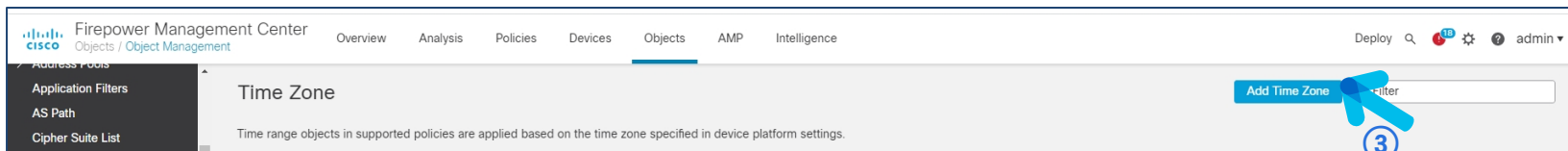
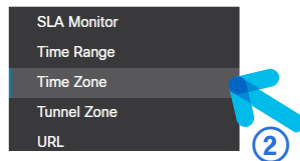
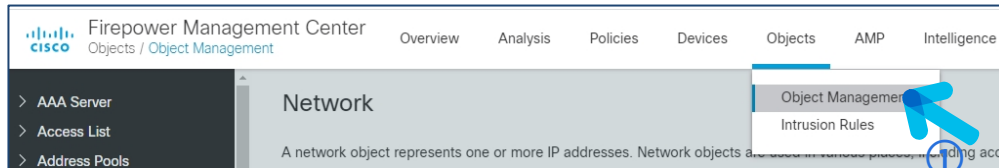
Time Range アクセス制御の設定

- Time Range によるアクセス制御機能を設定する。
- ここではオフィス内端末を想定した IP アドレス群を送信元とした通信を、平日の早朝と夜間、および土日終日の間ブロックする設定を行う。



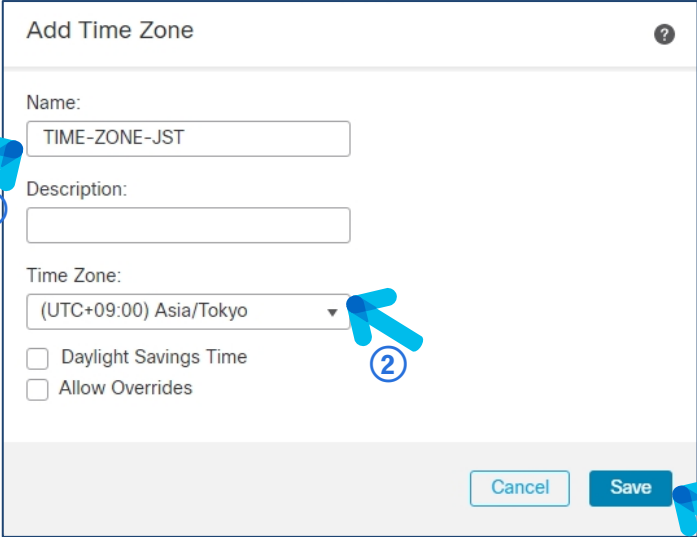
Time Zone の Object 設定

- FTD デバイスのタイムゾーンを、デフォルトの UTC から日本標準時間の JST へ変更する
- タイムゾーンの考え方は Firepower Management Center Configuration Guide, Version 7.0 の [Time Zone Object](#) を参照



- ① Objects 下の Object Management を選択
- ② 左側メニューより Time Zone を選択
- ③ Add Time Zone を選択

Time Zone の Object 設定



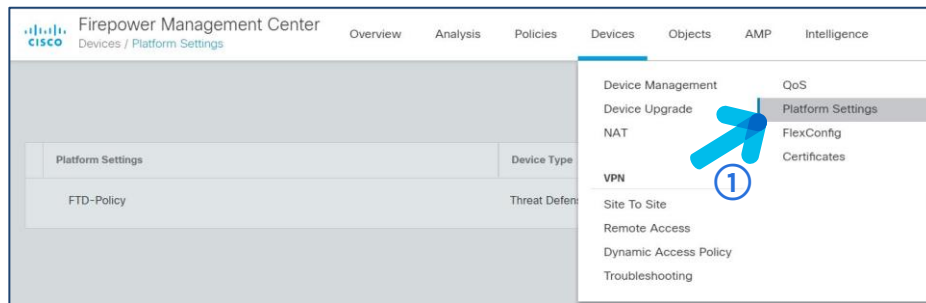
The screenshot shows a dialog box titled "Add Time Zone" with a help icon in the top right corner. It contains the following fields and controls:

- Name:** A text input field containing "TIME-ZONE-JST". A blue arrow with a circled "1" points to this field.
- Description:** An empty text input field.
- Time Zone:** A dropdown menu showing "(UTC+09:00) Asia/Tokyo". A blue arrow with a circled "2" points to the dropdown arrow.
- Daylight Savings Time
- Allow Overrides
- Buttons:** "Cancel" and "Save" buttons at the bottom right. A blue arrow with a circled "3" points to the "Save" button.

- ① Name を入力。本資料では "TIME-ZONE-JST" とする
- ② Time Zone にて (UTC + 9:00) Asia/Tokyo を選択する
- ③ Save をクリックする

Time Zone の適用

- 作成した Time Zone を FTD デバイスへ適用する



- ① Devices 下の Platform Settings を選択
- ② FMC 配下の FTD デバイスへ適用されている Platform Setting の編集アイコンをクリックする

Time Zone の適用

The screenshot shows the 'FTD-Policy' configuration page. On the left is a dark sidebar menu with various settings. The 'Time Zone' option is highlighted with a blue arrow and a circled '1'. The main content area has a 'Time Zone:' label above a dropdown menu showing 'TIME-ZONE-JST', which is also pointed to by a blue arrow and a circled '2'. Below the dropdown are three informational bullet points. In the top right corner, there are 'Save' and 'Cancel' buttons, with a blue arrow and a circled '3' pointing to the 'Save' button. A red text notification 'You have unsaved changes' is visible above the buttons. The text 'Policy Assignments (1)' is also present in the top right.

FTD-Policy
Enter Description

You have unsaved changes Save Cancel

Policy Assignments (1)

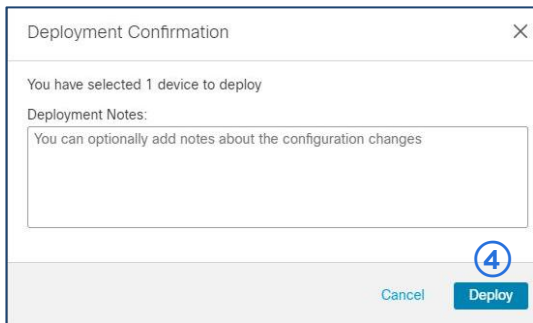
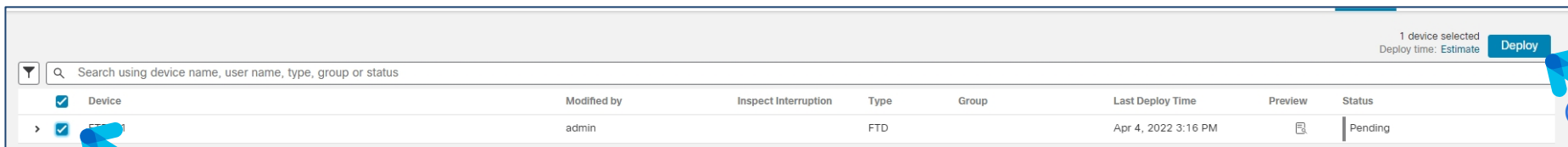
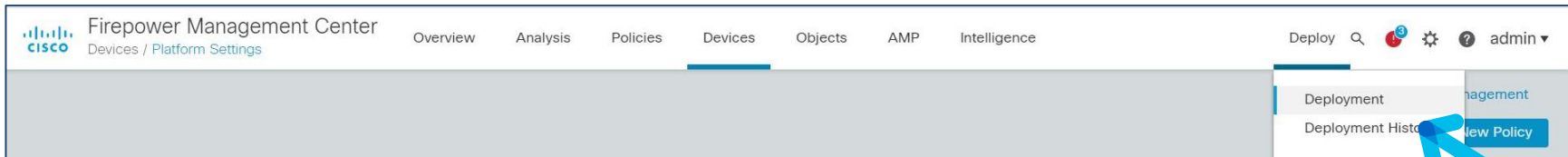
ARP Inspection
Banner
DNS
External Authentication
Fragment Settings
HTTP Access
ICMP Access
SSH Access
SMTP Server
SNMP
SSL
Syslog
Timeouts
Time Synchronization
Time Zone

Time Zone:
TIME-ZONE-JST

- 1 Time-based rules in supported policies are applied based on the time zone assigned to the device.
- 1 Time Zone setting is supported on FTD version 6.6.0 and above.
- 1 If no Time Zone is selected, Time Zone will be UTC Time Zone (UTC + 00:00).

- ① 左側メニューより Time Zone を選択
- ② Time Zone のプルダウンより、作成した Time Zone "TIME-ZONE-JST" を選択
- ③ Save をクリック

Time Zone の適用



- ① Deploy 下の Deployment をクリック
- ② Deploy 対象機器にチェックを入れる
- ③ 画面右上の Deploy をクリック
- ④ ポップアップウィンドウにて Deploy をクリック

Time Zone の適用

Firepower Management Center
Devices / NGFW Device Summary

Overview Analysis Policies **Devices** Objects AMP Intelligence

Deploy 🔍 ⚙️ ? admin ▾

FTDv01

Cisco Firepower Threat Defense for VMware

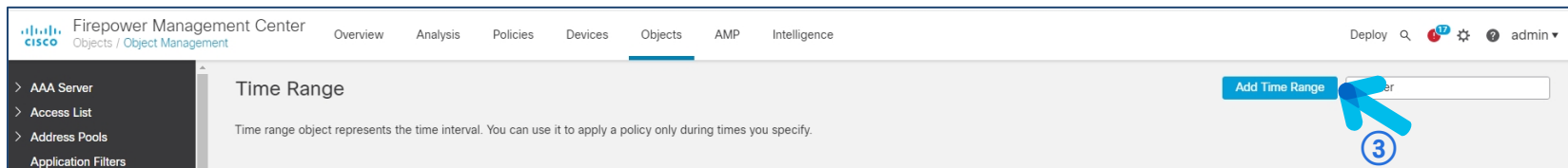
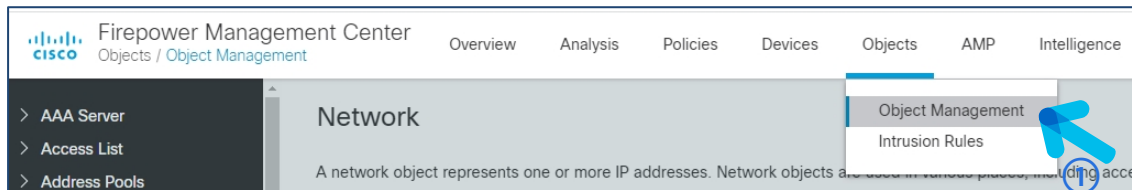
Device Routing Interfaces Inline Sets DHCP

General	License	System
Name: FTDv01	Performance Tier : FTDv - Variable	Model: Cisco Firepower Threat Defense for VMware
Transfer Packets: Yes	Base: Yes	Serial: 9A98KRRD4VS
Mode: Routed	Export-Controlled Features: Yes	Time: 2022-04-04 06:27:56
Compliance Mode: None	Malware: Yes	Time Zone: UTC (UTC+0:00)
TLS Crypto Acceleration: Disabled	Threat: Yes	Version: 7.0.1.1
	URL Filtering: Yes	Time Zone setting for Time based Rules: (UTC+09:00) Japan
	AnyConnect Apex: No	
	AnyConnect Plus: No	
	AnyConnect VPN Only: No	

- Deploy が完了すると、FTD デバイスの Time Zone setting for Time based Rules: が日本標準時間となっている。
※Devices > Device Management > 対象 FTDデバイス > Device タブより

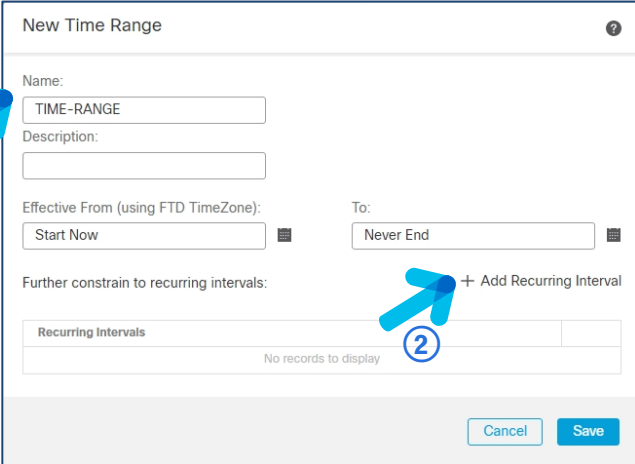
Time Range の Object 設定

- 平日の早朝と夜間、および土日終日に対応する Time Range Object を設定する。



- ① Objects 下の Object Management を選択
- ② 左側メニューより Time Range を選択
- ③ Add Time Range を選択

Time Range の Object 設定



New Time Range

Name:
TIME-RANGE

Description:

Effective From (using FTD TimeZone):
Start Now

To:
Never End

Further constrain to recurring intervals:
+ Add Recurring Interval

Recurring Intervals
No records to display

Cancel Save

- ① Name を入力。本資料では "TIME-RANGE" とする
- ② Add Recurring Interval をクリックする

Time Range の Object 設定

① Recurring Type: Daily Interval Range

② Days of Week: Mon Tue Wed Thu Fri Sat Sun

Daily

Effective Time (using FTD TimeZone):

From: 18:00

To: 23:59

All Day

Cancel Add

Recurring Type: Daily Interval Range

Days of Week: Mon Tue Wed Thu Fri Sat Sun

Daily

Effective Time (using FTD TimeZone):

From: 00:00

To: 08:00

All Day

Cancel Add

Recurring Type: Daily Interval Range

Days of Week: Mon Tue Wed Thu Fri Sat Sun

Daily

Effective Time (using FTD TimeZone):

From: 00:00

To: 23:59

All Day

Cancel Add

- ① まず平日夜間を定義する。Daily Interval を選択する
- ② Mon, Tue, Wed, Thu, Fri を選択する
- ③ Effective Time Zone に平日夜間を想定した時間として、18:00 ~ 23:59 を入力する
- ④ Add をクリック
- ⑤ 同様に平日早朝 (0:00 ~ 08:00) 相当する定義を画面のように設定し、Add をクリックする
- ⑥ 同様に土日終日に相当する定義を画面のように設定し、Add をクリックする

Time Range の Object 設定

Edit Time Range







Name:

Description:

Effective From (using FTD TimeZone):

To:

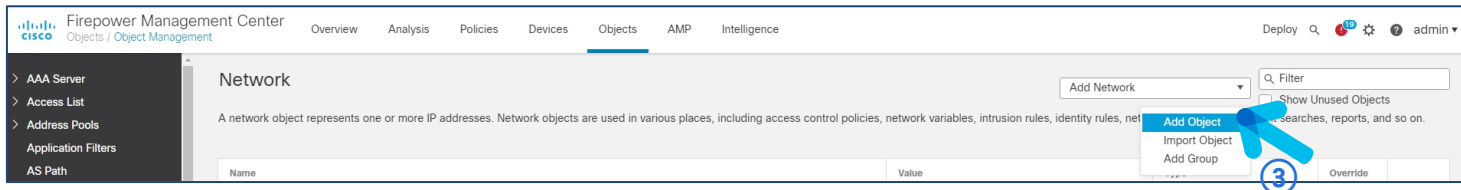
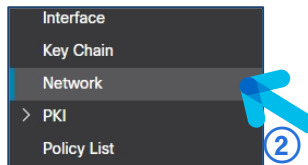
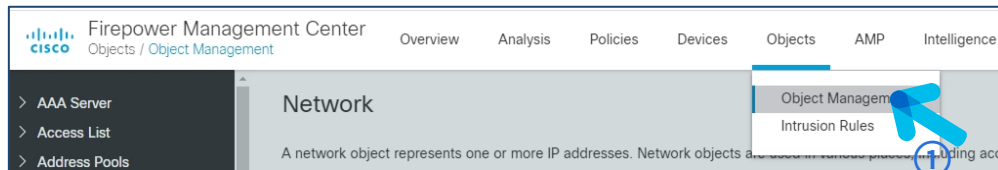
Further constrain to recurring intervals: [+ Add Recurring Interval](#)

Recurring Intervals	
Daily Interval: Weekdays, 18:00 to 23:59	 
Daily Interval: Weekdays, 00:00 to 08:00	 
Daily Interval: Weekend, 00:00 to 23:59	 

- ① Recurring Intervals に設定した三つの定義 (Weekdays, 18:00 to 23:59 / Weekdays, 00:00 to 8:00 / Weekend 00:00 to 23:59) が追加されたことを確認
- ② Save をクリック

オフィスを想定した Network Object 設定

- ・ オフィスを想定した Network Object を設定し、test PC1 の IP アドレス 192.168.1.101 を所属させる



- ① Objects 下の Object Management を選択
- ② 左側メニューより Network を選択
- ③ Add Network より Add Object を選択

オフィスを想定した Network Object 設定

New Network Object

Name
OFFICE

Description

Network
 Host Range Network FQDN

192.168.1.101

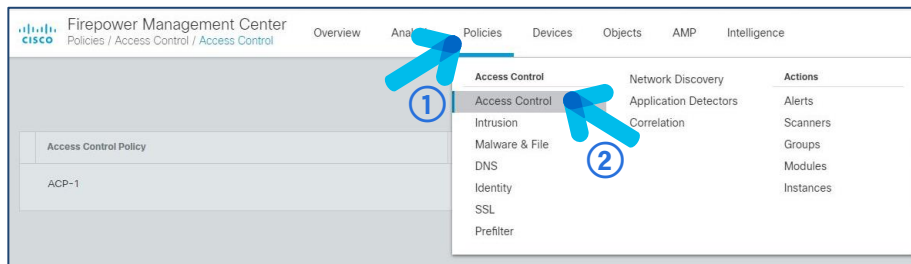
Allow Overrides



Cancel Save

- ① Name を入力。本資料では "OFFICE" とする
- ② Host を選択
- ③ テキストボックスに IP アドレス 192.168.1.101 を入力
- ④ Save をクリック

Time Range によるルール設定

- 作成した Time Range を用いたルールを設定する



Access Control Policy	Domain	Status	Last Modified	
ACP-1	Global	Targeting 1 devices Up-to-date on all targeted devices	2022-03-23 11:56:54 Modified by "Firepower System"	 



- 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“ACP-1”とする) の右側の鉛筆マークを選択

Time Range によるルール設定

The screenshot shows the configuration page for ACP-1. At the top, there are buttons for 'Show Warnings', 'Analyze Hit Counts', 'Save', and 'Cancel'. Below this is a tabbed interface with 'Rules', 'Intelligence', 'HTTP Responses', 'Logging', and 'Advanced'. The 'Rules' tab is selected and highlighted with a blue arrow and a circled '1'. To the right of the tabs, there are links for 'Inheritance Settings' and 'Policy Assignments (1)', and policy information: 'Prefilter Policy: Default Prefilter Policy', 'SSL Policy: None', and 'Identity Policy: None'. At the bottom, there is a search bar with 'Filter by Device' and 'Search Rules' text, a close button, a checkbox for 'Show Rule Conflicts', and a '+ Add Category' button. The '+ Add Rule' button is highlighted with a blue arrow and a circled '2'.

- ① Rules タブを選択
- ② Add Rule を選択

Time Range によるルール設定

Add Rule

Name: TIME-BASED (1) Enabled

Insert (3): above rule | 1

Action: Block (2)

Time Range: TIME-RANGE (4)

Zones Networks VLAN Tags Users Applications Ports URLs Dynamic Attributes Inspection Logging Comments

Available Zones

- External
- inside_zone
- Internal
- outside_zone

Source Zones (0): any

Destination Zones (0): any

- ① Name を入力。本資料では "TIME-BASED" とする
- ② Action のドロップダウンリストで、[Block] を選択
- ③ Insert のドロップダウンリストで [above rule] を選択し、テキストボックスへ [1] を入力
- ④ 使用する Time Range を選択する。ここでは作成済みの Object "TIME-RANGE" とする

Time Range によるルール設定

Add Rule

Name: TIME-BASED [Enabled] Move

Action: Block [Time Range: TIME-RANGE]

Zones Networks LAN Tags Users Applications Ports URLs Dynamic Attributes Inspection Logging Comments

Available Networks (1) Search by name or value

- IPV6-Private-Unique-Local-Addresses
- IPV6-to-IPv4-Relay-Anycast
- OFFICE**
- test-10.70.0.0/28
- test-10.70.66.0/28
- test-10.71.169.192
- test-172.16.0.0
- test-192.168.0.0-16

Source Networks (1) Source Original Client

- OFFICE

Destination Networks (0) any

Enter an IP address [Add] Enter an IP address [Add]

- ① Networks タブを選択
- ② Networks より OFFICE を選択
- ③ Add to Source Networks をクリック

Time Range によるルール設定

Add Rule

Name: TIME-BASED Enabled

Insert: above rule 1

Action: Block

Time Range: TIME-RANGE +

Zones Networks VLAN Tags Users Applications Ports URLs Dynamic Attributes Inspection **Logging** Comments

Log at Beginning of Connection **2**

Log at End of Connection

File Events:

Log Files

Send Connection Events to:

Firepower Management Center

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

SNMP Trap Select an SNMP Alert Configurat +

1

3

Cancel Add

- ① Logging タブを選択
- ② Log at Beginning of Connection にチェックを入れる
- ③ Add をクリック

Access Control Policy 保存と Deploy

The screenshot shows the Cisco Firepower Management Center interface for editing an Access Control Policy (ACP-1). The 'Policies' tab is active. A red notification 'You have unsaved changes' is visible. The 'Save' button is highlighted with a blue arrow and a circled '1'. Other buttons like 'Cancel', 'Analyze Hit Counts', and 'Inheritance Settings' are also visible. Below the main area, there are tabs for 'Rules', 'Security Intelligence', 'HTTP Responses', 'Logging', and 'Advanced'. A search bar and a table of rules are also present.

The screenshot shows the same Cisco Firepower Management Center interface, but now the 'Deploy' button is highlighted with a blue arrow and a circled '2'. A dropdown menu is open over the 'Deploy' button, showing options like 'Deployment History' and 'Deployment H...'. The 'Cancel' button is also visible. The 'Save' button is no longer highlighted.

- ① Save をクリック
- ② Deploy 下の Deployment をクリック

Access Control Policy 保存と Deploy

1 device selected
Deploy time: Estimate **Deploy**

Search using device name, user name, type, group or status

<input checked="" type="checkbox"/>	Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
<input checked="" type="checkbox"/>	FTDv01	admin		FTD		Apr 4, 2022 3:16 PM		Pending

Deployment Confirmation

You have selected 1 device to deploy

Deployment Notes:

You can optionally add notes about the configuration changes

- ① Deploy 対象機器にチェックを入れる
- ② 画面右上の Deploy をクリック
- ③ ポップアップウィンドウにて Deploy をクリック

Time Range アクセス制御のテスト

Firepower Management Center
Analysis / Connections / Events

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy admin

Jump to...

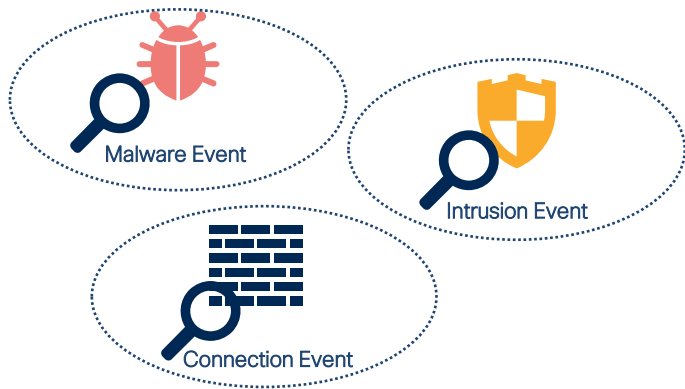
	<input type="checkbox"/>	↓ First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Web Application	URL	URL Category	URL Reputation	Device
▼	<input type="checkbox"/>	2022-04-04 18:01:50		Block		192.168.1.101		192.168.2.200		inside_zone	outside_zone	52073 / udp	53 (domain) / udp							FTDv01
▼	<input type="checkbox"/>	2022-04-04 18:01:50		Block		192.168.1.101		10.71.169.193		inside_zone	outside_zone	52073 / udp	53 (domain) / udp							FTDv01
▼	<input type="checkbox"/>	2022-04-04 18:01:47		Block		192.168.1.101		10.71.169.193		inside_zone	outside_zone	55004 / udp	53 (domain) / udp							FTDv01
▼	<input type="checkbox"/>	2022-04-04 18:01:47		Block		192.168.1.101		192.168.2.200		inside_zone	outside_zone	55004 / udp	53 (domain) / udp							FTDv01
▼	<input type="checkbox"/>	2022-04-04 18:01:35		Block		192.168.1.101		10.71.169.193		inside_zone	outside_zone	54751 / udp	53 (domain) / udp							FTDv01
▼	<input type="checkbox"/>	2022-04-04 18:01:34		Block		192.168.1.101		192.168.2.200		inside_zone	outside_zone	54751 / udp	53 (domain) / udp							FTDv01
▼	<input type="checkbox"/>	2022-04-04 18:01:12		Block		192.168.1.101		192.168.2.200		inside_zone	outside_zone	55442 / udp	53 (domain) / udp							FTDv01
▼	<input type="checkbox"/>	2022-04-04 18:01:12		Block		192.168.1.101		10.71.169.193		inside_zone	outside_zone	55442 / udp	53 (domain) / udp							FTDv01
▼	<input type="checkbox"/>	2022-04-04 18:00:50		Block		192.168.1.101		64.103.36.133	USA	inside_zone	outside_zone	1102 / tcp	8080 / tcp							FTDv01
▼	<input type="checkbox"/>	2022-04-04 18:00:46		Block		192.168.1.101		192.168.2.200		inside_zone	outside_zone	58828 / udp	53 (domain) / udp							FTDv01
▼	<input type="checkbox"/>	2022-04-04 18:00:46		Block		192.168.1.101		10.71.169.193		inside_zone	outside_zone	58828 / udp	53 (domain) / udp							FTDv01
▼	<input type="checkbox"/>	2022-04-04 18:00:39		Block		192.168.1.101		192.168.2.200		inside_zone	outside_zone	59584 / udp	53 (domain) / udp							FTDv01
▼	<input type="checkbox"/>	2022-04-04 18:00:39		Block		192.168.1.101		10.71.169.193		inside_zone	outside_zone	59584 / udp	53 (domain) / udp							FTDv01
▼	<input type="checkbox"/>	2022-04-04 18:00:35		Block		192.168.1.101		10.71.169.193		inside_zone	outside_zone	59345 / udp	53 (domain) / udp							FTDv01
▼	<input type="checkbox"/>	2022-04-04 18:00:34		Block		192.168.1.101		192.168.2.200		inside_zone	outside_zone	59345 / udp	53 (domain) / udp							FTDv01
▼	<input type="checkbox"/>	2022-04-04 18:00:32		Block		192.168.1.101		192.168.2.200		inside_zone	outside_zone	52267 / udp	53 (domain) / udp							FTDv01
▼	<input type="checkbox"/>	2022-04-04 18:00:32		Block		192.168.1.101		10.71.169.193		inside_zone	outside_zone	52267 / udp	53 (domain) / udp							FTDv01
▼	<input type="checkbox"/>	2022-04-04 18:00:21		Block		192.168.1.101		10.71.169.193		inside_zone	outside_zone	60695 / udp	53 (domain) / udp							FTDv01
▼	<input type="checkbox"/>	2022-04-04 18:00:21		Block		192.168.1.101		192.168.2.200		inside_zone	outside_zone	60695 / udp	53 (domain) / udp							FTDv01
▼	<input type="checkbox"/>	2022-04-04 18:00:15		Block		192.168.1.101		40.126.35.128	SGP	inside_zone	outside_zone	1101 / tcp	443 (https) / tcp							FTDv01
▼	<input type="checkbox"/>	2022-04-04 18:00:10		Block		192.168.1.101		192.168.2.200		inside_zone	outside_zone	55467 / udp	53 (domain) / udp		<input type="checkbox"/> DNS					FTDv01
▼	<input type="checkbox"/>	2022-04-04 18:00:10		Block		192.168.1.101		10.71.169.193		inside_zone	outside_zone	55467 / udp	53 (domain) / udp		<input type="checkbox"/> DNS					FTDv01
▼	<input type="checkbox"/>	2022-04-04 17:59:54	2022-04-04 18:00:25	Monitor		192.168.1.101		40.126.35.151	SGP	inside_zone	outside_zone	1100 / tcp	443 (https) / tcp							FTDv01
▼	<input type="checkbox"/>	2022-04-04 17:59:48	2022-04-04 18:00:18	Monitor		192.168.1.101		23.51.133.4	SGP	inside_zone	outside_zone	1099 / tcp	80 (http) / tcp							FTDv01
▼	<input type="checkbox"/>	2022-04-04 17:59:33	2022-04-04 18:00:03	Monitor		192.168.1.101		40.126.35.144	SGP	inside_zone	outside_zone	1098 / tcp	443 (https) / tcp							FTDv01

Page 4 of many > < | Displaying rows 76-100 of many rows

- 2022年4月4日(月) の Connection Event の確認結果。想定通りに 18:00 以降に開始した通信が、Block されていることがわかる

Unified Events とは

- Unified Event 画面は複数種別のイベントを一つのビューで参照できるイベント調査画面
- 例えばマルウェアイベントと IPS イベントの関連性調査や、通信ログのリアルタイムな効果確認において有用なビュー
- バージョン 7.0.0 より追加された



Firepower Management Center

Overview Analysis Policies Devices Objects AMP Intelligence

Showing 104 events (1/104)

Time	Event Type	Action	Source IP	Destination IP	Source Port / XMAP Type	Destination Port / Application	Access Control Rule	Access Control Policy
2022-04-12 17:59:56	Connection	Allow	192.168.1.101	13.107.21.200	4943 / tcp		CATCH-ALL_URL-MONITOR	ACP-1
2022-04-12 17:54:08	Connection	Allow	192.168.1.101	13.107.42.16	4943 / tcp		URL-MONITOR_CATCH-ALL	ACP-1
2022-04-12 17:54:09	Connection	Allow	192.168.1.101	202.232.2.39	53829 / tcp		CATCH-ALL_URL-MONITOR	ACP-1
2022-04-12 17:54:09	Connection	Allow	192.168.1.101	50.80.209	4941 / tcp	443 (https) / tcp	URL-MONITOR_CATCH-ALL	ACP-1
2022-04-12 17:54:09	Connection	Allow	192.168.1.101	202.232.2.39	80 (http) / tcp	53 (domain) / udp	URL-MONITOR_CATCH-ALL	ACP-1
2022-04-12 17:54:09	Connection	Allow	192.168.1.101	40.90.194.62	4940 / tcp	443 (https) / tcp	CATCH-ALL_URL-MONITOR	ACP-1
2022-04-12 17:54:09	Connection	Allow	192.168.1.101	154.16.24.243	48959 / tcp	80 (http) / tcp	OCSP	ACP-1

1011010
1011010
1011010
1011010

Unified Event

Unified Events とは

Firepower Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects AMP Intelligence

Showing all 682 events (🔍 631 📌 5 📄 36 🚩 10) ↓

Time	Event Type	Action
2022-04-12 10:39:13	File	Malware B
2022-04-12 10:39:13	Malware	Malware B
2022-04-12 10:39:12	Connection	Block
2022-04-12 10:39:12	Connection	Block
2022-04-12 10:39:12	Connection	Monitor
2022-04-12 10:39:12	File	Malware B
2022-04-12 10:39:12	Malware	Malware B
2022-04-12 10:39:11	File	Malware B
2022-04-12 10:39:11	Malware	Malware B
2022-04-12 10:39:10	Connection	Monitor
2022-04-12 10:39:10	File	Malware B
2022-04-12 10:39:10	Malware	Malware B
2022-04-12 10:39:08	Connection	Block
2022-04-12 10:39:08	Connection	Block

- ① Analysis を選択
- ② Unified Events を選択

Unified Events とは

検索ボックス

Live viewへの切り替えボタン。
FTD デバイスが検知したログを、
リアルタイムで表示するモード

The screenshot shows the Firepower Management Center interface for Unified Events. A search bar is highlighted with a red box and a blue arrow pointing to the text '検索ボックス'. A 'Go Live' button is highlighted with a red box and a blue arrow pointing to the text 'Live viewへの切り替えボタン...'. A table of events is shown with a blue arrow pointing to the 'Time' column header, which is annotated with 'カラム編集ボタン。クリックするとビューで表示するカラムを編集できる'. Another blue arrow points to a date range filter in the table header, annotated with '表示対象とする期間の設定。クリックし、表示対象期間を変更可能'. The table contains columns for Time, Event Type, Action, Reason, Source IP, Destination IP, Source Port / ICMP Type, Destination Port / ICMP Code, Web Application, Access Control Rule, and Access Control Policy.

Time	Event Type	Action	Reason	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Web Application	Access Control Rule	Access Control Policy
2022-04-12 17:59:56	Connection	Allow		192.168.1.101	13.107.21.200	49943 / tcp	443 (https) / tcp	Bing	CATCH-ALL, URL-MONITOR	ACP-1
2022-04-12 17:54:09	Connection	Allow		192.168.1.101	13.107.21.200	49943 / tcp	443 (https) / tcp	Bing	URL-MONITOR, CATCH-ALL	ACP-1
2022-04-12 17:51:51	Connection	Allow		192.168.1.101	202.232.2.39	60164 / udp	53 (domain) / udp		URL-MONITOR, CATCH-ALL	ACP-1
2022-04-12 17:51:51	Connection	Allow		192.168.1.101	40.90.184.82	49940 / tcp	443 (https) / tcp	Microsoft	CATCH-ALL, URL-MONITOR	ACP-1
2022-04-12 17:51:51	Connection	Allow		192.168.1.101	104.18.24.243	49939 / tcp	80 (http) / tcp	OCSP	URL-MONITOR, CATCH-ALL	ACP-1
2022-04-12 17:51:51	Connection	Allow		192.168.1.101	202.232.2.38	58988 / udp	53 (domain) / udp		CATCH-ALL, URL-MONITOR	ACP-1
2022-04-12 17:51:51	Connection	Allow		192.168.1.101	202.232.2.39	58988 / udp	53 (domain) / udp		CATCH-ALL, URL-MONITOR	ACP-1
2022-04-12 17:51:51	Connection	Allow		192.168.1.101	40.90.184.82	49938 / tcp	443 (https) / tcp	Microsoft	URL-MONITOR, CATCH-ALL	ACP-1
2022-04-12 17:51:50	Connection	Allow		192.168.1.101	23.35.192.53	49935 / tcp	443 (https) / tcp	Exchange Online	URL-MONITOR, CATCH-ALL	ACP-1
2022-04-12 17:51:50	Connection	Allow		192.168.1.101	23.35.192.53	49934 / tcp	443 (https) / tcp	Exchange Online	CATCH-ALL, URL-MONITOR	ACP-1
2022-04-12 17:51:50	Connection	Allow		192.168.1.101	23.35.192.53	49933 / tcp	443 (https) / tcp	Exchange Online	URL-MONITOR, CATCH-ALL	ACP-1

Unified Events による調査

- 例として、特定の時間帯でホスト 192.168.1.101 をターゲットとして検出された Intrusion イベント、Malware イベントを検索する
- Time Range : 2022年4月12日 10:00:00 ~ 11:00:00
- Destination IP : 192.168.1.101
- Event Type : Intrusion、Malware

Unified Events による調査

Firepower Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy 🔍 ⚙️ ? admin ▾

Showing all 104 events (t3, 104) ↓

🕒 2022-04-12 17:01:18 JST - 2022-04-12 17:59:59 JST 58m 41s Go Live

Fixed Time Range Sliding Time Range

Start time End time Now

2022-04-12 10 : 00 : 00 2022-04-12 11 : 00 : 00

Select last: 5 minutes, 6 hours, 1 day, 2 weeks, 1 month

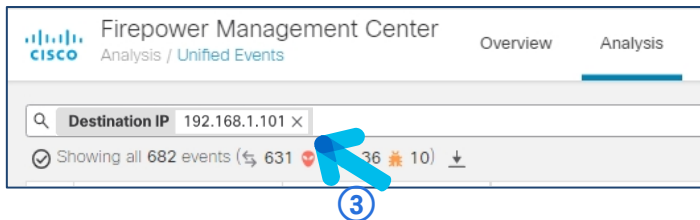
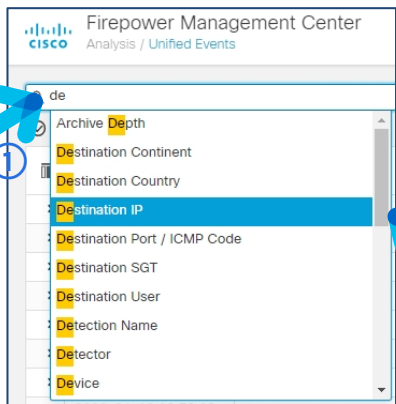
April 2022 April 2022

Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

1h selected Apply

- ① Time Range をクリック
- ② Start Time を 2022-04-12 10:00:00 へ設定
- ③ End Time を 2022-04-12 11:00:00 へ設定
- ④ Apply をクリック

Unified Events による調査



- ① 検索ボックスに [de] と入力
- ② 候補より Destination IP を選択
- ③ テキストボックスへ 192.168.1.101 と入力

Unified Events による調査

Firepower Management Center
Analysis / Unified Events

Overview Analysis Policies Devices

Destination IP 192.168.1.101 x x Event Type Intrusion x Malware x x

Showing all 682 events (63 5 36 10) ①

Showing:

- all 631 connection events
- all 5 intrusion events
- all 36 file events
- all 10 malware events

Tip: **ctrl** +click an event type to add to filter, **alt** +click to exclude from filter. The same works on data in the table below.

	Reason

Firepower Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy Search Settings Help admin

Destination IP 192.168.1.101 x x Event Type Intrusion x Malware x x

Showing all 682 events (631 5 36 10) ↓

2022-04-12 10:00:00 JST → 2022-04-12 11:00:00 JST 1h

Apply Cancel

- ① Ctrlキー をクリックしながら、intrusion event、malware event のアイコンをクリックする
- ② Apply をクリック

Unified Events による調査

Firepower Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy 🔍 ⚙️ ? admin ▼

Destination IP 192.168.22.161 × Event Type Intrusion × Malware × × Refresh

Showing all 12 events (🔴 2 🟡 10) ↓ 2022-04-12 10:00:00 JST → 2022-04-12 11:00:00 JST 1h Go Live

Time	Event Type	Action	Reason	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Web Application	Access Control Rule	Access Control Policy	Device
> 2022-04-12 10:52:12	Intrusion	Would have dropped	Intrusion Policy in "Detection"	10.70.83.22	192.168.1.101	110 (pop3) / tcp	14688 / tcp		CATCH-ALL	ACP-1	FTDv01
> 2022-04-12 10:47:54	Intrusion	Would have dropped	Intrusion Policy in "Detection"	10.70.83.22	192.168.1.101	110 (pop3) / tcp	14588 / tcp		CATCH-ALL	ACP-1	FTDv01
> 2022-04-12 10:39:34	Malware	Malware Block		64.103.36.133	192.168.1.101	8080 / tcp	1221 / tcp	HTTP Tunnel			FTDv01
> 2022-04-12 10:39:32	Malware	Malware Block		64.103.36.133	192.168.1.101	8080 / tcp	1219 / tcp	HTTP Tunnel			FTDv01
> 2022-04-12 10:39:32	Malware	Malware Block		64.103.36.133	192.168.1.101	8080 / tcp	1218 / tcp	HTTP Tunnel			FTDv01
> 2022-04-12 10:39:31	Malware	Malware Block		64.103.36.133	192.168.1.101	8080 / tcp	1217 / tcp	HTTP Tunnel			FTDv01
> 2022-04-12 10:39:19	Malware	Malware Block		64.103.36.133	192.168.1.101	8080 / tcp	1196 / tcp	HTTP Tunnel			FTDv01
> 2022-04-12 10:39:18	Malware	Malware Block		64.103.36.133	192.168.1.101	8080 / tcp	1192 / tcp	HTTP Tunnel			FTDv01
> 2022-04-12 10:39:13	Malware	Malware Block		64.103.36.133	192.168.1.101	8080 / tcp	1191 / tcp	HTTP Tunnel			FTDv01
> 2022-04-12 10:39:12	Malware	Malware Block		64.103.36.133	192.168.1.101	8080 / tcp	1188 / tcp	HTTP Tunnel			FTDv01
> 2022-04-12 10:39:11	Malware	Malware Block		64.103.36.133	192.168.1.101	8080 / tcp	1187 / tcp	HTTP Tunnel			FTDv01
> 2022-04-12 10:39:10	Malware	Malware Block		64.103.36.133	192.168.1.101	8080 / tcp	1186 / tcp	HTTP Tunnel			FTDv01



① フィルタした結果が表示される。各イベントの詳細は >アイコンをクリックすると表示される

Unified Events による調査

Time	Event Type	Action	Reason	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Web Application	Access Control Rule	Access Control Policy
2022-04-12 10:52:12	Intrusion	Would have dropped	Intrusion Policy in "Detection"	10.70.83.22	192.168.1.101	110 (pop3) / tcp	14688 / tcp		CATCH-ALL	ACP-1
<p>Event Type: Intrusion</p> <p>Time: 2022-04-12 10:52:12</p> <p>Priority: high</p> <p>Impact: Impact 1</p> <p>Action: Would have dropped</p> <p>Reason: Intrusion Policy in "Detection" Inspection Mode</p> <p>Source IP: 192.168.1.101</p> <p>Destination IP: 192.168.22.161</p> <p>Source Port / ICMP Type: 110 (pop3) / tcp</p> <p>Destination Port / ICMP Code: 14688 / tcp</p> <p>SSL Status: Unknown (Unknown)</p> <p>VLAN ID: 0</p> <p>MPLS Label: 0</p> <p>Intrusion Message: MALWARE-OTHER.PUA.Win.File.Zegost-9629018-0 dow...</p> <p>Classification: A Network Trojan was Detected</p> <p>Generator: Standard Text Rule</p> <p>Source User: Unknown</p> <p>Destination User: Discovered Identities(sysadmin2 (POP3))</p> <p>Application Protocol: POP3</p> <p>Application Protocol Category: email</p> <p>Application Protocol Tag: allows remote connect</p> <p>Client Application: POP3</p> <p>Client Application Category: email</p> <p>Client Application Tag: allows remote connect</p> <p>Application Risk: Medium</p> <p>Business Relevance: High</p> <p>Ingress Security Zone: outside_zone</p> <p>Egress Security Zone: inside_zone</p> <p>Domain: Global</p> <p>Device: FTDv01</p> <p>Ingress Interface: outside</p> <p>Egress Interface: inside</p> <p>Ingress Virtual Router: Global</p> <p>Egress Virtual Router: Global</p> <p>Intrusion Policy: INTRUSION_POLICY</p> <p>Access Control Policy: ACP-1</p> <p>Access Control Rule: CATCH-ALL</p> <p>Network Analysis Policy: Balanced Security and Connectivity</p> <p>HTTP Response Code: 0</p> <p>Reviewed By: Unreviewed</p>										

- Unified Event における Intrusion Event の詳細表示例。

Unified Events による調査

2022-04-12 10:39:34	Malware	Malware Block	64.103.36.133	192.168.1.101	8080 / tcp	1221 / tcp	HTTP Tunnel		
Event Type: Malware Time: 2022-04-12 10:39:34 Action: Malware Block Source IP: 64.103.36.133 Source Country: USA Destination IP: 192.168.1.101 Source Port / ICMP Type: 8080 / tcp Destination Port / ICMP Code: 1221 / tcp SSL Status: Decrypt (Resign) Source User: Not Found Malware Event Type: Threat Detected in Network File Transfer Detection Name: EICAR File Name: secure.eicar.org:443	Disposition: Malware SHA-256: 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2... Threat Score: Very High File Type: EICAR Category: Executables Size (KB): 0.066 URL: http://secure.eicar.org:443 Application Protocol: HTTP Application Protocol Category: network protocols/services Application Protocol Tag: file sharing/transfer, encrypted visibility engine, allows rem... Client Application: Chrome Client Application Category: web browser Client Application Tag: encrypts communications, recent vulnerabilities, SSL proto...	Web Application: HTTP Tunnel Web Application Category: network protocols/services, vpn/tunnel Web Application Tag: tunnels Application Risk: High Business Relevance: Medium Detector: SHA File Policy: File Detection Policy Domain: Global Device: FTDv01 Ingress Virtual Router: Global Egress Virtual Router: Global							

- Unified Event における Malware Event の詳細表示例。



The bridge to possible