Cisco Start

Cisco ASA Firepower モジュール

かんたんセットアップ ガイド

本ガイドの手順で ASA Firepower モジュールを
かんたんにセットアップできます

1. 事前設定
2. セキュリティ ポリシーの設定
3. データベースの更新
4. レポーティングとモニタリング

CISCO

1 事前設定

1-1 はじめに

本ガイドでは、Cisco ASA 搭載の「Cisco ASA Firepower モジュール」による、ネットワーク トラフィックを制御するための基本的なセキュリティ（アクセス コントロール）ポリシーを設定します。別冊の『**Cisco ASA with Firepower Services かんたんセットアップ ガイド**』などを参考に、ライセンスのインストールまでの初期セットアップを完了してから、本ガイドの設定を開始してください。設定には、Cisco Adaptive Security Device Manager（ASDM）を使用します。

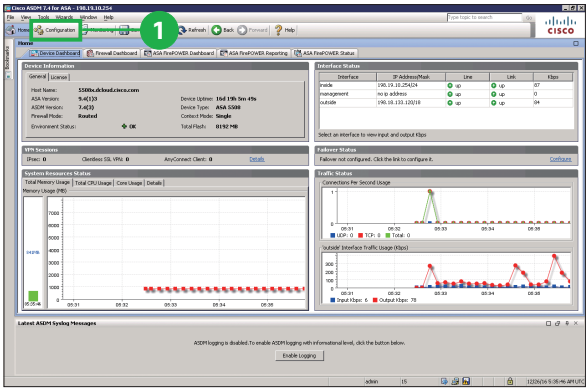
また、本ガイドの一部の設定では、オプション ライセンスがインストール済みであることを前提としています。その場合には「MEMO」「注意」コラムなどで、必要なライセンスを明記しています。Cisco ASA with Firepower Services には、デフォルトで **Application Visibility and Control**（AVC）ライセンスが付属していますが、オプションの **Next-Generation IPS**（NGIPS）、**Cisco Advanced Malware Protection**（AMP）、および **URL フィルタリング**（URL）ライセンスを購入することで、さらに高度な機能を追加できます。

- **AVC**：3,000 を超えるアプリケーションの識別および制御機能が使用できます。
- **NGIPS**：きわめて効果的な脅威保護と、ユーザ、インフラストラクチャ、アプリケーション、およびコンテンツに対するフル コンテキスト認識機能を備え、マルチベクトルな脅威も検出し、防御対策を自動化します。
- **AMP**：高度なマルウェアに対してインライン ネットワーク保護および Cisco Threat Grid サンドボックスを提供します。
- **URL**：2.8 億以上のトップレベルのドメインをリスク レベルごとに 82 以上のカテゴリにフィルタリングできます。

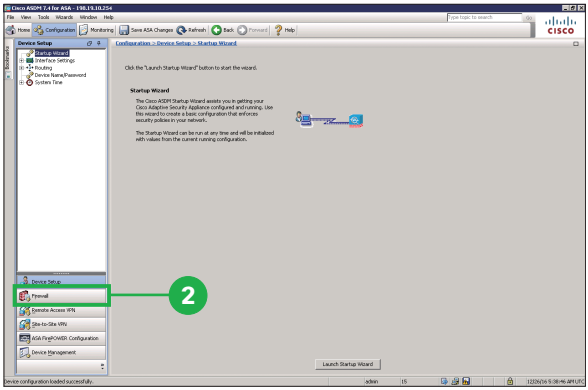
オプション ライセンス	SKU に含まれる文字列	NGIPS	AMP	URL
NGIPS ライセンス	TA	●	-	-
AMP ライセンス	AMP	-	●	-
URL ライセンス	URL	-	-	●
NGIPS & AMP ライセンス	TAM	●	●	-
NGIPS & URL ライセンス	TAC	●	-	●
NGIPS & AMP & URL ライセンス	TAMC	●	●	●

1-2 サービス ポリシーの設定

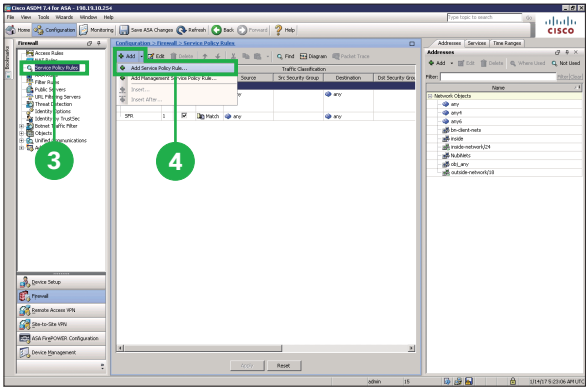
ASA Firepower モジュールにネットワーク トラフィックをリダイレクトするためのサービス ポリシーを設定します。ASDM を起動します。



1 [Configuration] をクリック

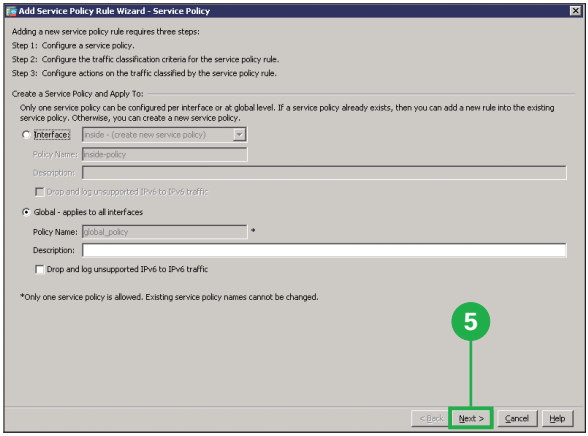


2 [Firewall] をクリック



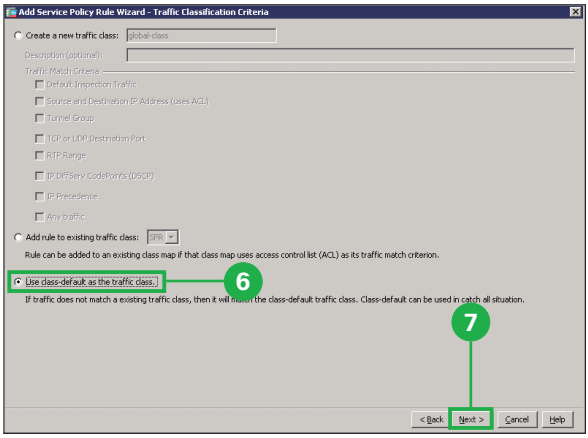
3 [Service Policy Rules] をクリック

4 [Add] メニューから [Add Service Policy Rule] を選択



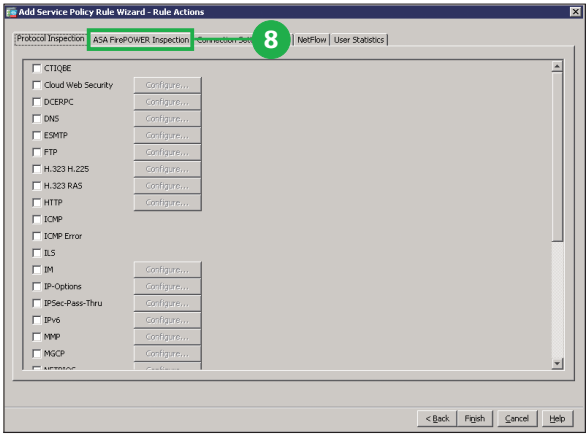
5 [Next] をクリック

デフォルトで選択されている [Global - applies to all interfaces] は変更せずに [Next] をクリックします。

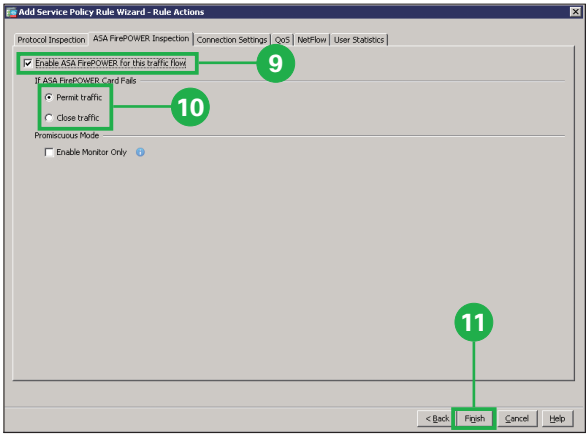


6 [Use class-default as the traffic class] をクリック

7 [Next] をクリック



8 [ASA FirePOWER Inspection] をクリック



9 [Enable ASA FirePOWER for this traffic flow] をクリック

10 [Permit traffic]または[Close traffic] をクリック

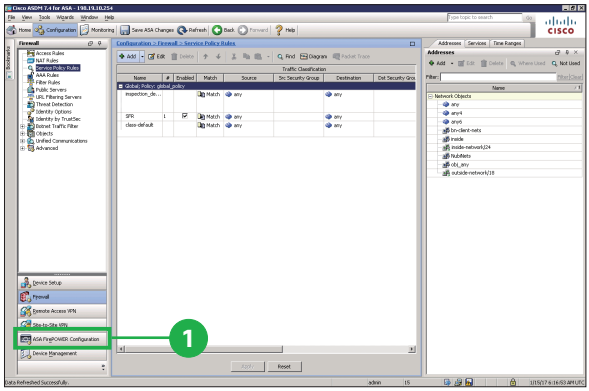
障害が発生した場合など、ASA Firepower モジュールが利用不可能な場合の動作を選択します。[Permit traffic] を選択した場合、すべてのネットワーク トラフィックを検知なしで通過させます。[Close traffic]を選択した場合、すべてのネットワーク トラフィックを遮断します。

11 [Finish] をクリック

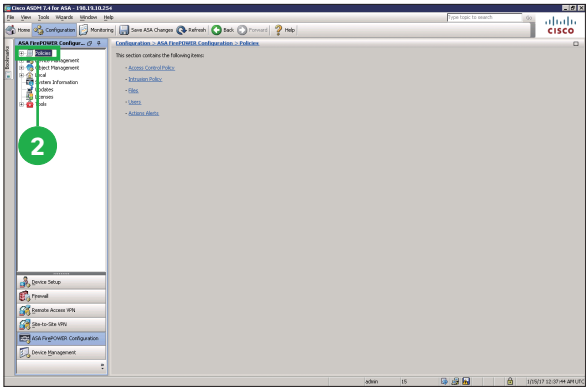
2 セキュリティ ポリシーの設定

2-1 ファイル ポリシーの設定：マルウェア対策

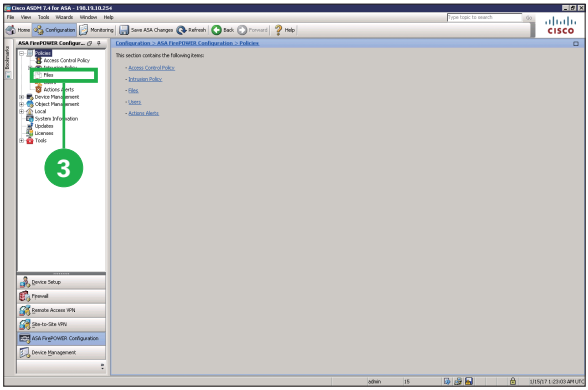
マルウェア対策として、ユーザがアップロード（送信）またはダウンロード（受信）するファイルの検知やブロックなど、特定の種類のファイルをコントロールするためのファイル ポリシーを設定します。ここで設定するファイル ポリシーは「**2-2　アクセス コントロール ポリシーの設定：可視化**」で使用します。



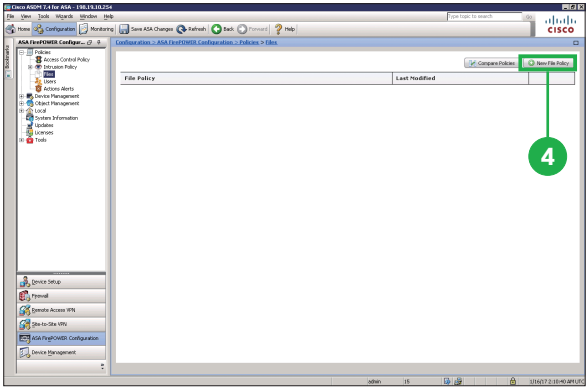
1 ［ASA FirePOWER Configuration］をクリック



2 ［Policies］をクリック

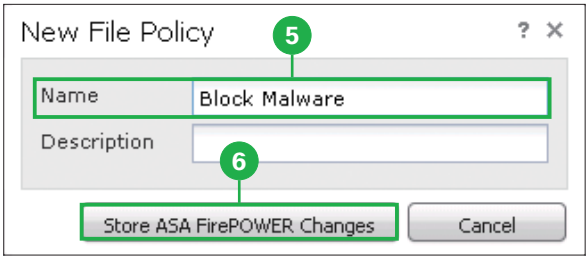


3 [Files] をクリック



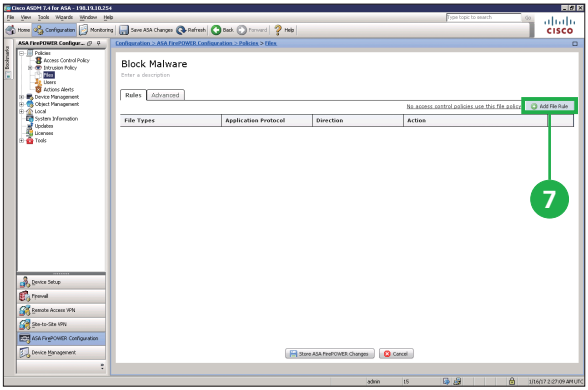
4 [New File Policy] をクリック

[New File Policy] ポップアップ ウインドウが表示されます。



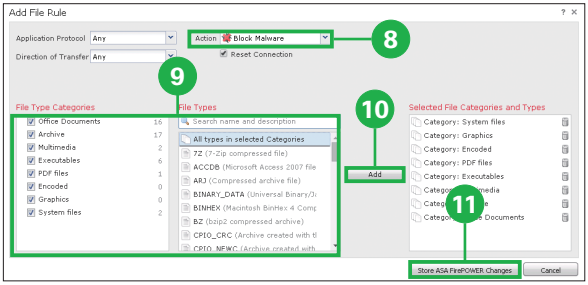
5 [Name] 欄に任意のポリシー名を入力

6 [Store ASA FirePOWER Changes] をクリック



7 ［Add File Rule］をクリック

［Add File Rule］ポップアップ ウインドウが表示されます。



8 ［Action］メニューから［Block Malware］を選択

9 マルウェアを検知およびブロックしたいファイルの種類を選択

10 ［Add］をクリック

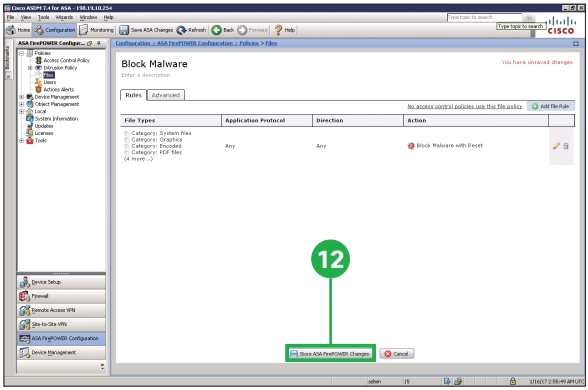
ファイルの種類はカテゴリ別に選択、および種類別に検索と選択が可能です。

11 ［Store ASA FirePOWER Changes］をクリック

⚠ 注意

❽で選択できる［Malware Cloud Lookup］または［Block Malware］設定が実際に機能するためにはNGIPS ライセンスまたは AMP ライセンスが必要です。これらのライセンスをインストールしていない場合は［Detect Files］または［Block Files］を選択してください。

- **Detect Files**：❾で選択した種類のファイルを検知します。
- **Block Files**：❾で選択した種類のファイルをブロックします。
- **Malware Cloud Lookup**：❾で選択した種類のファイルに対してマルウェア検査を実行します。
- **Block　Malware**：❾で選択した種類のファイルに対してマルウェア検査を実行し、脅威の疑いがある場合にはブロックします。



12 [Store ASA FirePOWER Changes] をクリック

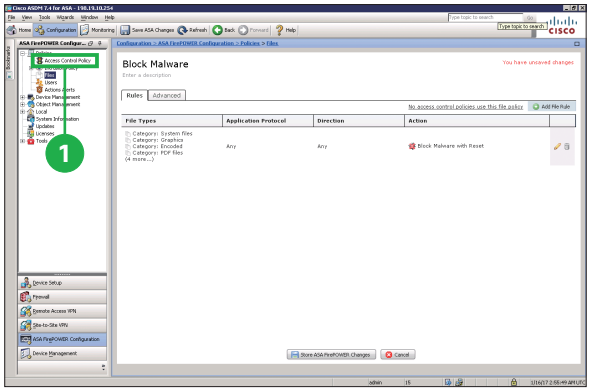
[Apply Access Control Policy]ポップアップ ウインドウが表示されます。

MEMO

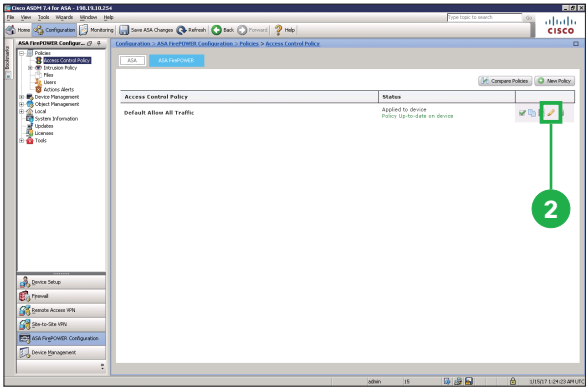
ファイル ポリシーには、複数のルールを設定できます。ファイルの種類のカテゴリ別や種類別にルールを設定する場合は、❼から⓫の手順をくり返してルールを追加します。

2-2 アクセス コントロール ポリシーの設定：可視化

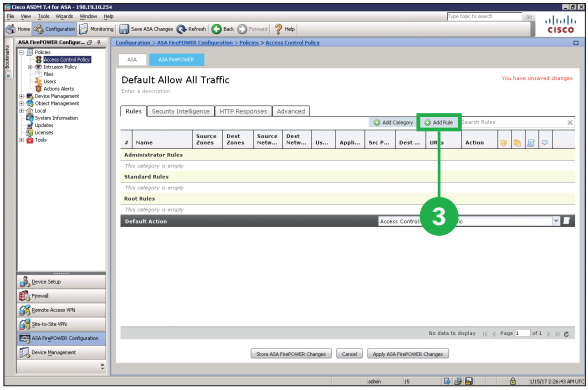
デフォルトの［Default Allow All Traffic］ポリシーを編集して、ネットワーク トラフィックを可視化（ロギングおよびモニタリング）するためのルールを設定します。



1 ［Access Control Policy］をクリック

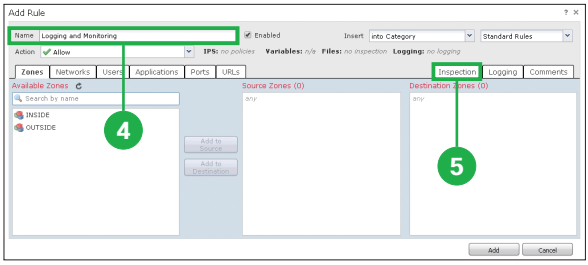


2 ［Default Allow All Traffic］ポリシーのペン アイコン（ ）をクリック



3 ［Add Rule］をクリック

［Add Rule］ポップアップ ウインドウが表示されます。



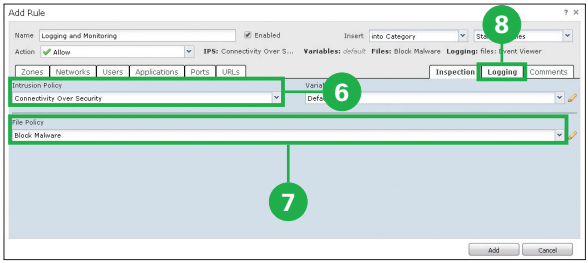
4 ［Name］欄に任意のルール名を入力

5 ［Inspection］タブをクリック

侵入防御ポリシーおよびファイル ポリシーの設定画面が表示されます。

⚠ 注意

❻で選択できる侵入防御ポリシー設定が実際に機能するためには NGIPS ライセンスが必要です。ライセンスをインストールしていない場合は［None］を選択してください。



6 ［Intrusion Policy］メニューから［Connectivity Over Security］を選択

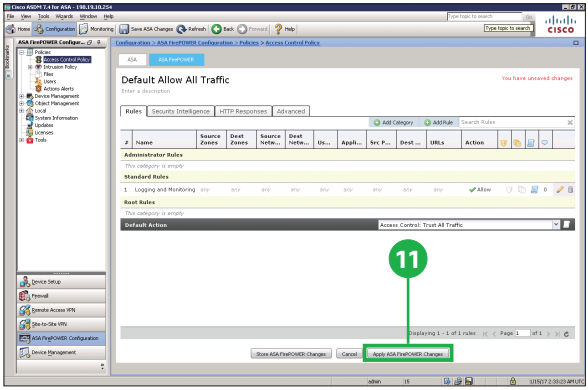
7 ［File Policy］メニューから「2-1 ファイル ポリシーの設定：マルウェア対策」❺で入力したポリシー名を選択

8 ［Logging］タブをクリック

ログの設定画面が表示されます。

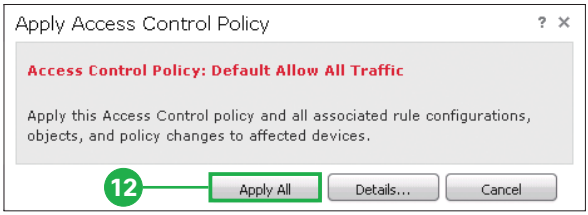
9 ［Log at End of Connection］をクリック

10 ［Add］をクリック



11 ［Apply ASA FirePOWER Changes］をクリック

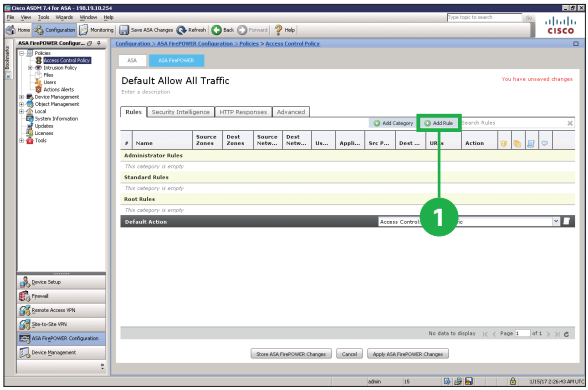
[Apply Access Control Policy]ポップアップ ウインドウが表示されます。



12 ［Apply All］をクリック

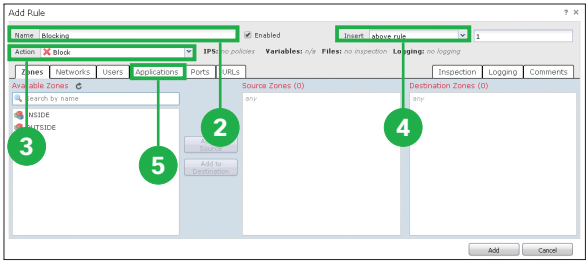
2-3 アクセス コントロール ポリシーの設定：ブロック

デフォルトの［Default Allow All Traffic］ポリシーではすべてのネットワーク トラフィックが通過するため、業務に関係がないアプリケーションの利用や危険な URL へのアクセスを禁止したい場合など、特定のネットワーク トラフィックをブロックするためのルールを設定します。



1 ［Add Rule］をクリック

［Add Rule］ポップアップ ウインドウが表示されます。



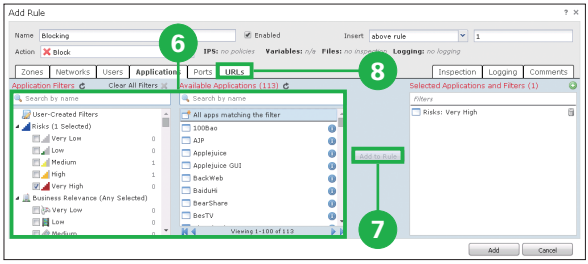
2 ［Name］欄に任意のルール名を入力

3 ［Action］メニューから［Block］を選択

4 ［Insert］メニューから［above rule］を選択

5 ［Applications］タブをクリック

アプリケーションの選択画面が表示されます。



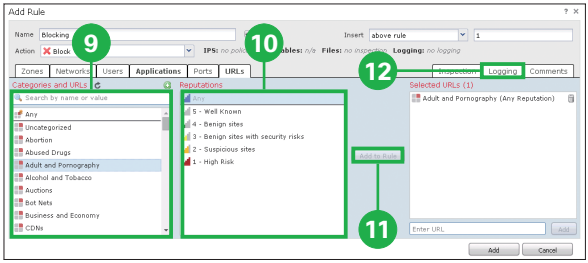
6 利用を禁止したいアプリケーションを選択

7 ［Add to Rule］をクリック

アプリケーションはグループ別および個別に検索と選択が可能です。

8 ［URL］タブをクリック

URL の選択画面が表示されます。



9 アクセスを禁止したい URL カテゴリを選択

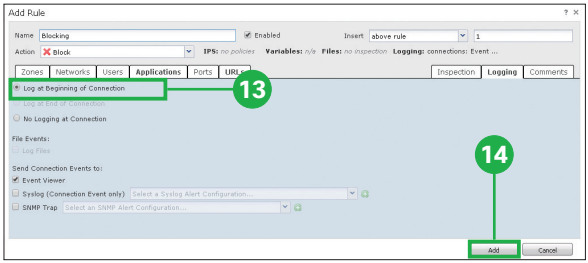
10 アクセスを禁止したい URL レピュテーションを選択

11 ［Add to Rule］をクリック

URL はカテゴリ別に検索と選択、およびレピュテーション別に選択が可能です。

12 ［Logging］タブをクリック

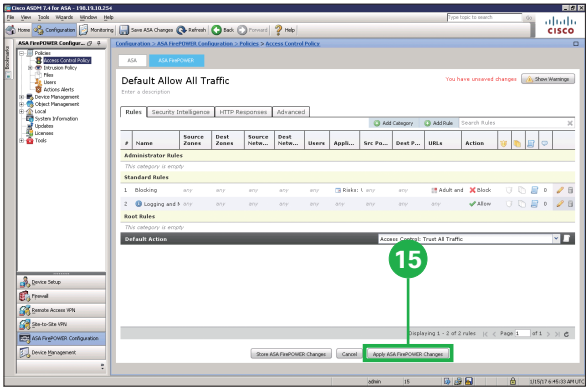
ログの設定画面が表示されます。



13 ［Log at Beginning and End of Connection］をクリック

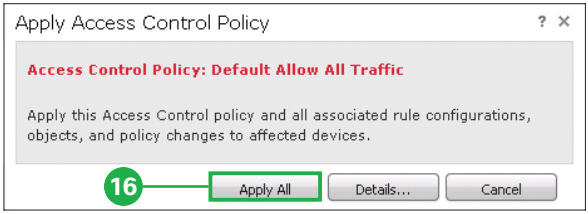
14 ［Add］をクリック

> ⚠ **注意**
>
> ⑩で選択できる URL レピュテーションが実際に機能するためには URL ライセンスが必要です。



15 [Apply ASA FirePOWER Changes] をクリック

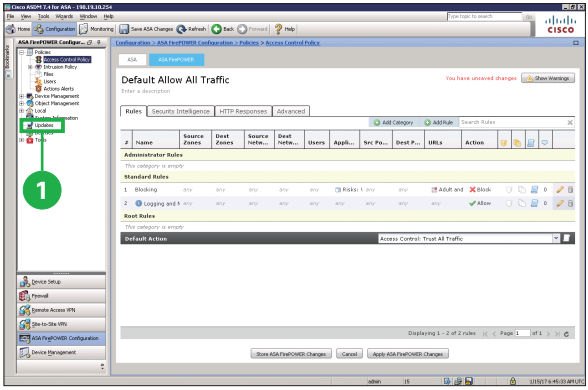
[Apply Access Control Policy]ポップアップ ウインドウが表示されます。



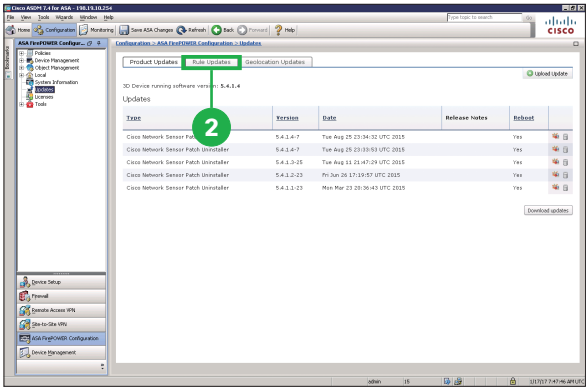
16 [Apply All] をクリック

3 データベースの更新

新たな脅威が発見されるたびに、シスコはセキュリティ データベースを更新しています。定期的なデータベース更新を設定して、常に最新のデータベースに基づいてネットワークを保護できるようにします。

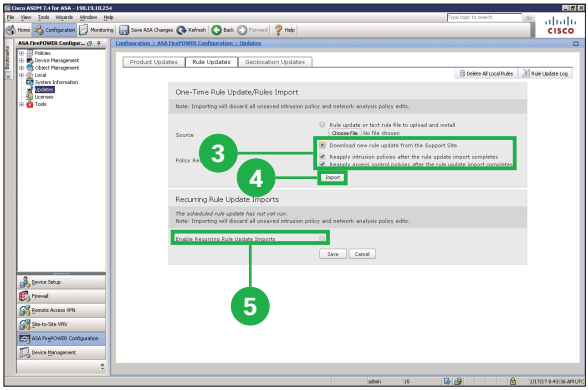


1 [Updates] をクリック



2 [Rule Updates] タブをクリック

ルール データベース更新の設定画面が表示されます。



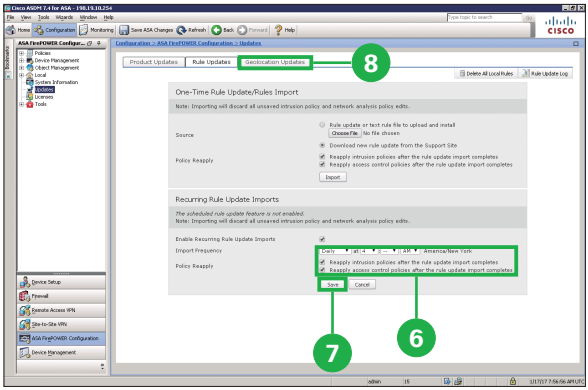
3 ［Download new Rule Update from the Support Site］を選択して、その下の 2 つのオプションをクリック

4 ［Import］をクリック

最新のルール データベースに更新されます。

5 ［Enable Recurring Rule Update Imports］をクリック

設定オプションが表示されます。



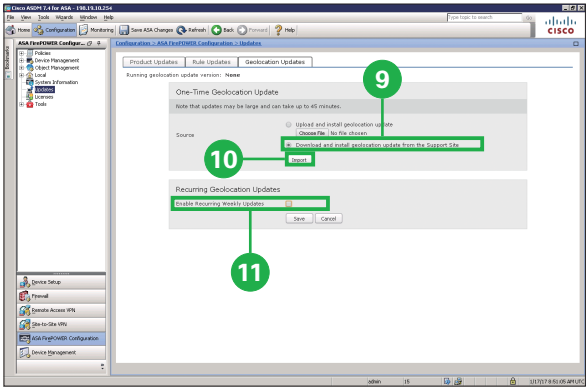
6 自動更新間隔を設定して、その下の 2 つのオプションをクリック

デフォルトの［Daily］が推奨です。

7 ［Save］をクリック

8 ［Geolocation Updates］タブをクリック

地理位置情報データベース更新の設定画面が表示されます。



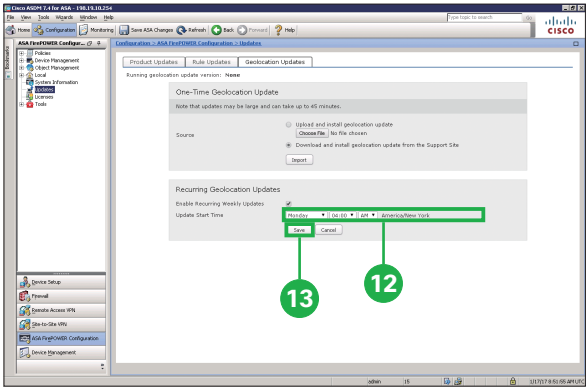
9 ［Download and install geolocation update from the Support Site］をクリック

10 ［Import］をクリック

最新の地理位置情報データベースに更新されます。

11 ［Enable Recurring Weekly Updates］をクリック

設定オプションが表示されます。



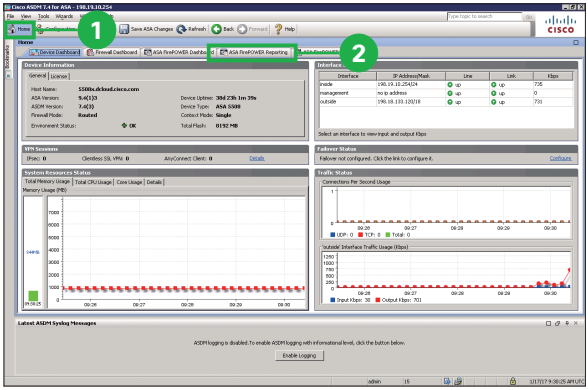
12 自動更新曜日を設定

13 ［Save］をクリック

4 レポーティングとモニタリング

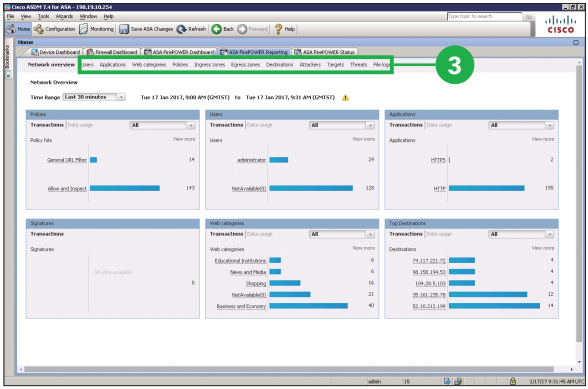
Cisco ASDM はネットワークの管理に役立つ、数々の強力なレポーティングおよびモニタリング機能を備えています。ASA Firepower モジュールに関するレポーティングおよびモニタリング ページにアクセスして、「**2　セキュリティ ポリシーの設定**」で設定した内容が機能している様子をグラフィカルに確認してみましょう。

4-1 レポーティング ページにアクセスする



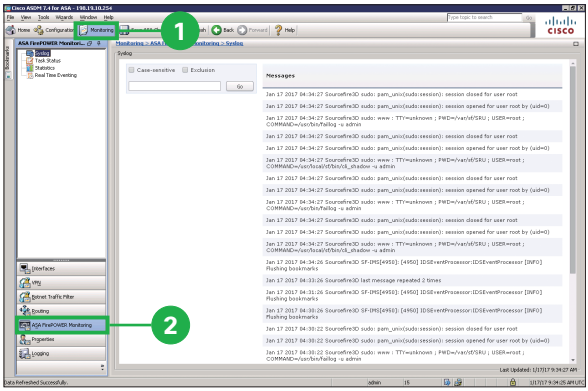
1 ［Home］をクリック

2 ［ASA FirePOWER Reporting］をクリック



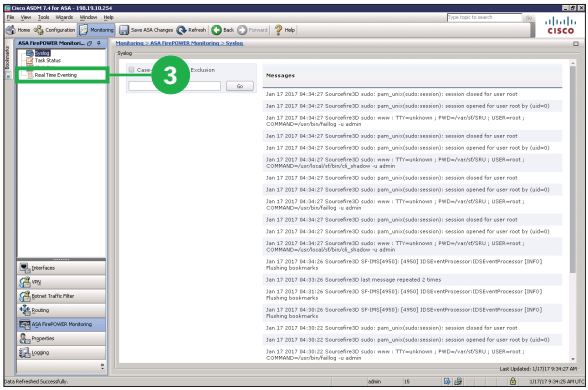
3 表示したいレポート内容をクリック

4-2 モニタリング ページにアクセスする

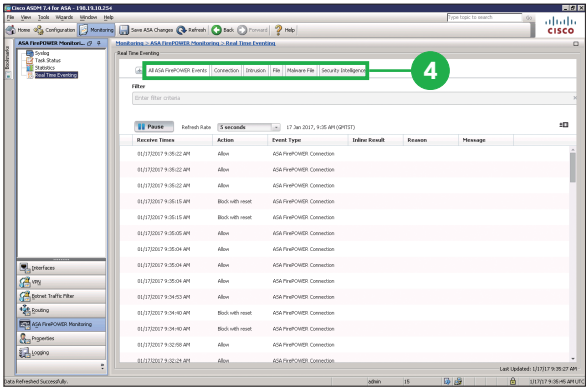


1 ［Monitoring］をクリック

2 ［ASA FirePOWER Monitoring］をクリック



3 ［Real Time Eventing］をクリック



4 表示したいモニタ内容をクリック

お問い合わせ方法

電話または E メールにてお問い合わせください。

Cisco Start テクニカル サポート総合受付窓口

電 話 **0120-092-255**

「ご希望の番号を選択してください」という自動音声ガイダンスの後、
電話機のプッシュ番号 **3 番**
（製品 / サービスご購入後の技術的なサポートについてのお問い合わせ）を押します。
続いて **7 番（シスコ スタート）**を押してください。
最後に **3 番（ワイヤレス製品）**を選択してください。

E メール **start-jp@cisco.com**

受付時間：平日 午前 9 時～午後 18 時（土日祝日は休み）
※時間外のお問い合わせは翌営業日の受付となります。

製品サポート期間：購入元にご確認ください。
ご返答までの目安：受付後、翌営業日までに担当エンジニアよりご連絡いたします。
※5 営業日を目安に復旧策 / 回避策をご提供いたします。

お問い合わせに必要な情報

お問い合わせの際には、以下の情報をご用意ください。
E メールでお問い合わせの際には、こちらのテキストと必要事項を記入して送信してください。

＜ご担当者情報＞
- ご担当者のお名前（漢字/ふりがな）：
- Cisco.com ID：
- 会社名（漢字/ふりがな）：
- 住所（漢字/ふりがな）：
- 電話番号：
- FAX 番号：
- E メール アドレス：

＜製品情報＞
- シリアル番号：
- 問題の内容：
- 製品設置先住所（漢字/ふりがな）：
- サービス契約番号（お持ちの場合のみ）：

お問い合わせ先

シスコシステムズ合同会社
〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

1291-1706-02A-TO