ASA with FirePOWER Services の使用開始

Cisco ASA FirePOWER モジュールは、一部の Cisco ASA 5500-X シリーズ アプライアンスに展開できます。詳細については、*Cisco FirePOWER* 互換性ガイドを参照してください。モジュールは、ユーザ組織のセキュリティ ポリシーに準拠した方法でネットワーク トラフィックを処理するように設計されています。

このガイドでは、Adaptive Security Device Manager（ASDM）を使用してアクセス可能な ASA FirePOWER モジュールの機能の設定方法について説明します。

また、Firepower Management Center を使用した ASA with FirePOWER Services デバイスの管理方法については、*Cisco Firepower Management Center* コンフィギュレーション ガイドを参照してください。

- クイック スタート：基本設定 （1 ページ）
- ASA With FirePOWER Services デバイス （5 ページ）
- ASA With FirePOWER Services の機能 （5 ページ）
- Firepower のオンラインヘルプ、ハウツー、およびドキュメント （7 ページ）
- Firepower システムの IP アドレス表記法 （10 ページ）
- 関連リソース （10 ページ）

クイック スタート：基本設定

ASA with FirePOWER Services デバイスの設定を開始する場合は、Cisco ASA FirePOWER モジュール クイック スタート ガイドを参照してください。クイック スタート ガイドには、以下を含む、セットアップ プロセス全体の説明が含まれています。

1. ASA with FirePOWER Services の導入。

（注） ASDM を使用して ASA with FirePOWER Services を管理するための Firepower Management Center への ASA with FirePOWER Services の登録セクションはスキップします。

⚠

注意 Firepower Management Center または ADSM を使用して、特定のアプライアンスを管理できますが、両方を使用することはできません。管理方式を切り替えると、既存のアプライアンスの設定が削除されます。

2. ASDM の開始。
3. ASA with FirePOWER Services の設定。

ポリシーと基本設定の設定

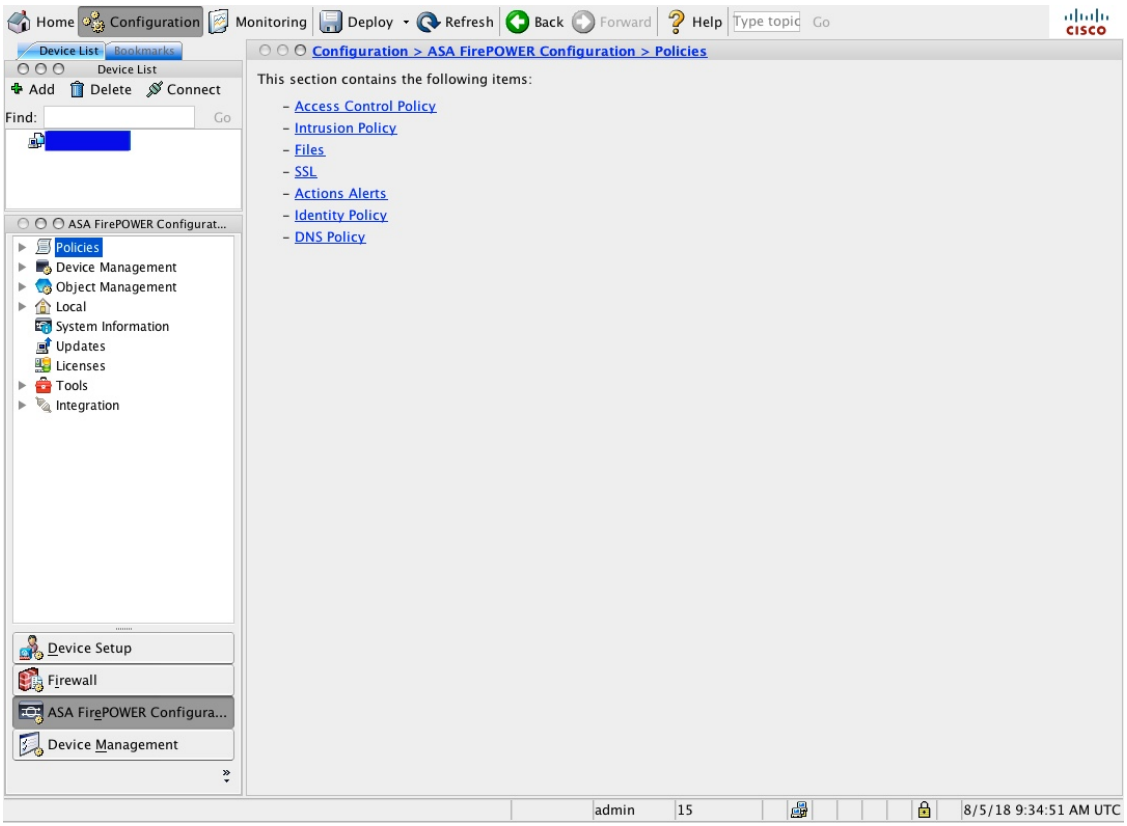
始める前に

クイック スタート：基本設定 （1 ページ）の説明に従い、最初に ASA with FirePOWER Services モジュールを設定します。

ステップ 1 クイック スタート ガイドの説明に従い、ASDM を起動して、ASA with FirePOWER Services モジュールにログインします。

ステップ 2 上部のナビゲーション バーで、[Configuration] をクリックします。

ステップ 3 サイドのナビゲーション バーで、[ASA FirePOWER Configuration] をクリックします。
次のような [Configuration] ページが表示されます。

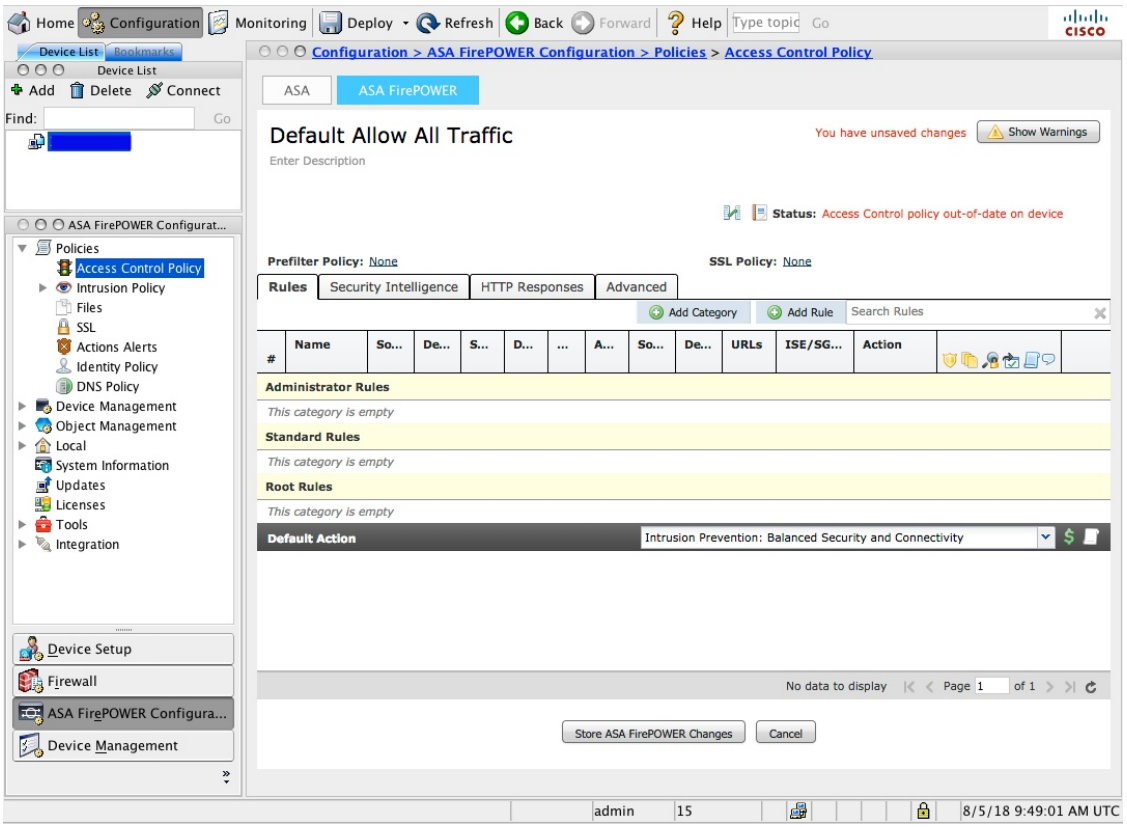


ステップ 4 基本的なアクセス コントロール ポリシーの作成の説明に従い、アクセス コントロール ポリシーを作成します。

a) [Policies] を展開します。

b) [Access Control Policy] をクリックします。

c) [ASA with FirePOWER] をクリックします。
次のような [Policy] ページが表示されます。



d) ほとんどの場合、[Default Action] では、[Intrusion Prevention: Balanced Security and Connectivity] を選択することをお勧めします。

ステップ 5 その他の共通の設定をカスタマイズします。

a) デバイス インターフェイスの管理
b) システム ポリシーの設定
c) ローカル設定の設定
d) Advanced Malware Protection を使用する場合、クラウド通信の有効化
e) 外部のアラートを使用した Syslog サーバまたは SNMP データへのログのストリーミング
f) バックアップのスケジュール
g) ソフトウェアの自動ダウンロードのスケジュール
h) ソフトウェアの自動インストールのスケジュール
i) ルールの自動更新のスケジュール
j) URL フィルタリングの自動更新のスケジュール
k) 地理位置情報データベースの自動更新のスケジュール

次のタスク

Cisco Adaptive Security Device Manager コンフィギュレーション ガイドの説明に従い、ASA オプションを設定します。

ASA With FirePOWER Services デバイス

ASA with FirePOWER Services デバイスは、次世代侵入防御システム（NGIPS）デバイスと呼ばれることもあります。これらのデバイスは、ASA デバイス上で NGIPS ソフトウェアを実行します。

ASA デバイスは最も重要なシステム ポリシーを提供し、検出およびアクセス コントロールのためにトラフィックを ASA FirePOWER モジュールに渡します。

ASA FirePOWER には ASA プラットフォームに固有のユーザ インターフェイスとコマンド ライン インターフェイス（CLI）があります。これらの ASA 固有のツールを使用して、システムをインストールしたり、プラットフォーム固有の他の管理タスクを実行したりすることができます。

ASA FirePOWER は次の Firepower 機能をサポートしていません。

- Firepower ハードウェアの機能：ASA CLI および ASDM を使用して、デバイスのハイ アベイラビリティ、スタッキング、スイッチング、ルーティング、VPN、NAT などを設定します。詳細については、ASA のマニュアルを参照してください。
- インターフェイスの設定：Firepower Management Center の Web インターフェイスを使用して ASA FirePOWER インターフェイスを設定することはできません。ASA FirePOWER が SPAN ポート モードで展開されている場合、Firepower Management Center には ASA インターフェイスは表示されません。
- プロセス管理：Firepower Management Center を使用して、ASA FirePOWER プロセスのシャットダウン、再起動、その他の管理を行うことはできません。

ASA With FirePOWER Services の機能

このセクションでは、一般的に使用される ASA With FirePOWER Services の機能をいくつか示します。

アプライアンスおよびシステム管理の機能

不明なドキュメントを探す場合は、ドキュメント ロードマップを参照してください。

目的	設定	参照場所
アプライアンスのデータをバックアップする	バックアップと復元	バックアップと復元の使用
新しいソフトウェア バージョンへのアップグレード	ソフトウェア アップデート	ASA FirePOWER モジュール ソフトウェアの更新

目的	設定	参照場所
アプライアンスを基準に合わせる	工場出荷時の初期状態に復元（再イメージ化）する	• Cisco ASA および Firepower Threat Defense 再イメージ化ガイド • Cisco Adaptive Security Device Manager コンフィギュレーション ガイドの FirePOWER モジュールの再イメージ化に関するセクション
アプライアンスの動作の継続性を確保する	ハイ アベイラビリティ	Cisco Adaptive Security Device Manager Configuration Guides
VDB を更新する、侵入ルールを更新する、またはアプライアンスの GeoDB を更新する	脆弱性データベース（VDB）の更新、侵入ルールの更新、地理位置情報データベース（GeoDB）の更新	更新のタイプについて
ライセンス制御機能を利用するためにライセンスを適用する	移行が可能	ライセンスについて
複数のインターフェイス間のトラフィックをルーティングするようにデバイスを設定する	ルーティング	ASDM コンフィギュレーション ガイド
インターネット接続のプライベート アドレスをパブリック アドレスに変換する	ネットワーク アドレス変換（NAT）	Cisco Adaptive Security Device Manager Configuration Guides

潜在的な脅威を検出、防御、および処理するための機能

不明なドキュメントを探す場合は、ドキュメント ロードマップを参照してください。

目的	設定	参照場所
ネットワーク トラフィックのインスペクション、記録、およびアクションを実行する	アクセス コントロール ポリシー、他のいくつかのポリシーの親	アクセス コントロール ポリシーの開始
IP アドレス、URL、またはドメイン名との間の接続をブロックする	アクセス コントロール ポリシー内のセキュリティ インテリジェンス	セキュリティ インテリジェンス戦略の選択

目的	設定	参照場所
ネットワーク上の悪意のあるトラフィックと侵入をモニタする	侵入ポリシー	侵入ポリシーについて
インスペクションを実行せずに、暗号化されたトラフィックをブロックする 暗号化または複合されたトラフィックのインスペクション	SSL ポリシー	トラフィック復号の概要
ネットワーク上のファイルを許可またはブロックする	ファイル ポリシー	侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御
ユーザの認知およびユーザ制御を実行するためにパッシブまたはアクティブなユーザ認証を設定する	ユーザ認識、ユーザ アイデンティティ、アイデンティティ ポリシー	アイデンティティ データの概要

外部ツールとの統合

不明なドキュメントを探す場合は、ドキュメント ロードマップを参照してください。

目的	設定	参照場所
カスタム開発されたクライアント アプリケーションにイベント データをストリーミングする	eStreamer 統合	高度なデバイス設定について

Firepowerのオンラインヘルプ、ハウツー、およびドキュメント

オンライン ヘルプには、Web インターフェイスからアクセスできます。

- 各ページで状況依存ヘルプのリンクをクリックする。
- **[Help]** > **[Online]** を選択する。

ハウツーは、Firepower Management Center 上でタスク間を移動するためのウォークスルーを提供するウィジェットです。ウォークスルーでは、タスクを実行するために移動する必要があるかもしれない各種 UI 画面かどうかを問わず、各ステップを順次体験することでタスクを完遂

するために必要なステップを実行します。デフォルトで [How To] ウィジェットは有効になっています。ウィジェットを無効にするには、ユーザ名の下にあるドロップダウンリストから [User Preferences] を選択し、[How-To Settings] にある [Enable How-Tos] チェックボックスをオフにします。

（注） 通常、ウォークスルーはすべての UI ページで利用でき、ユーザ ロールは区別されていません。ただし、ユーザの権限によっては Firepower Management Center のインターフェイスに表示されないメニュー項目もあります。そのため、そのようなページではウォークスルーは実行されません。

Firepower Management Center では次のウォークスルーを使用できます。

- [Cisco スマート アカウントへの FMC の登録（Register FMC with Cisco Smart Account）]：このウォークスルーでは、Cisco スマート アカウントに Firepower Management Center を登録する手順について説明します。
- [デバイスのセットアップと FMC への追加（Set up a Device and add it to FMC）]：このウォークスルーでは、デバイスをセットアップし、そのデバイスを Firepower Management Center に追加する手順について説明します。
- [日付と時刻の設定（Configure Date and Time）]：このウォークスルーでは、プラットフォーム設定ポリシーを使用して Firepower Threat Defense デバイスの日付と時刻を設定する手順について説明します。
- [インターフェイスの設定（Configure Interface Settings）]：このウォークスルーでは、Firepower Threat Defense デバイス上のインターフェイスを設定する手順について説明します。
- [アクセス コントロール ポリシーの作成（Create an Access Control Policy）]：アクセス コントロール ポリシーは上から下へと評価される、順序付けられた一連のルールから構成されています。このウォークスルーでは、アクセス コントロール ポリシーを作成する手順について説明します。
- [アクセス コントロール ルールの追加（Add an Access Control Rule）] - 機能のウォークスルー：このウォークスルーでは、アクセス コントロール ルールのコンポーネントと、Firepower Management Center でのそれらの使用方法について説明します。
- [ルーティングの設定（Configure Routing Settings）]：Firepower Threat Defense ではさまざまなルーティング プロトコルがサポートされています。スタティック ルートは、特定の宛先ネットワークのトラフィックの送信先を定義します。このウォークスルーでは、デバイスのスタティック ルーティングを設定する手順について説明します。
- [NAT ポリシーの作成（Create a NAT Policy）] - 機能のウォークスルー：このウォークスルーでは、NAT ポリシーを作成する手順とともに、NAT ルールのさまざまな機能について説明します。

ドキュメントのロードマップを使用して Firepower システムに関連する他のドキュメントについてはhttp://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html を参照してください。

関連資料

このセクションに記載されているドキュメントは、ASA with FirePOWER Services アプライアンスを設定する際に役立つことがあります。

ハードウェア ガイドとデータシート

次のガイドには、ASA with FirePOWER Services ハードウェアに関する詳細な情報が記載されています。

- https://www.cisco.com/c/en/us/support/security/asa-firepower-services/tsd-products-support-series-home.html
- https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html
- https://www.cisco.com/c/en/us/td/docs/security/asa/quick_start/sfr/firepower-qsg.html

詳細情報

一部のトピックは、Firepower Management Center コンフィギュレーション ガイドで詳細に説明されているため、このガイドには含まれていません。次の表に、このガイドで詳細情報が説明されていないトピックを示します。以下も参照してください。 関連資料 （9 ページ）

詳細情報の項目	FMC コンフィギュレーション ガイドのパート > 章を参照
アクセス コントロール ルール	**Access Control** > **Access Control Rules**
侵入ポリシー	**Intrusion Detection and Prevention** > **Getting Started with Intrusion Policies**
トラブルシューティング ツール	**System Monitoring and Troubleshooting** > **Troubleshooting the System**
ユーザ制御用のレルム	**Discovery and Identity** > **Create and Manage Realms**
アイデンティティ ポリシー	**Discovery and Identity** > **Create and Manage Identity Policies**
内部認証局（CA）	**Deployment Management** > **Reusable Objects**
信頼できる CA	**Deployment Management** > **Reusable Objects**
地理位置情報データベースの更新	**Deployment Management** > **Reusable Objects**

ドキュメント内のサポート対象デバイスに関する記述

章または項目の先頭に記載されているサポート対象デバイスに関する記述は、ある機能が特定のデバイス シリーズ、ファミリ、またはモデルでのみサポートされていることを示しています。たとえば、多くの機能は Firepower Threat Defense デバイスのみでサポートされています。

このリリースでサポートされているプラットフォームの詳細については、リリース ノートを参照してください。

ドキュメント内のアクセス ステートメント

このドキュメントの各手順の先頭に記載されているアクセス ステートメントは、手順の実行に必要な事前定義のユーザ ロールを示しています。記載されている任意のロールを使用して手順を実行することができます。

カスタム ロールを持っているユーザは、事前定義されたロールとは異なる権限セットを持つことができます。事前定義されたロールを使用して手順のアクセス要件が示されている場合は、同様の権限を持つカスタム ロールにもアクセス権があります。カスタム ロールを持っているユーザは、設定ページにアクセスするために使用するメニューパスが若干異なる場合があります。たとえば、侵入ポリシー権限のみが付与されているカスタム ロールを持つユーザは、アクセス コントロール ポリシーを使用する標準パスではなく侵入ポリシーを経由してネットワーク分析ポリシーにアクセスします。

Firepower システムの IP アドレス表記法

IPv4 Classless Inter-Domain Routing（CIDR）の表記、および IPv6 と同様のプレフィックス長の表記を使用して、Firepower システムのさまざまな場所でアドレス ブロックを定義することができます。

CIDR またはプレフィックス長の表記を使用して IP アドレスのブロックを指定する場合、Firepower システムは、マスクまたはプレフィックス長で指定されたネットワーク IP アドレスの部分**のみ**を使用します。たとえば、10.1.2.3/8 と入力した場合、Firepower システムでは 10.0.0.0/8 が使用されます。

つまり、Cisco では CIDR またはプレフィックス長の表記を使用する場合に、ビット境界上でネットワーク IP アドレスを使用する標準の方法を推奨していますが、Firepower システムではこれは必要ありません。

関連リソース

ファイアウォール コミュニティは、参考資料の包括的リポジトリで、シスコの広範にわたるドキュメンテーションを補完します。これには、シスコのハードウェアの3Dモデル、ハードウェア構成セレクタ、製品販促アイテム、設定例、トラブルシューティングに関するテクニカル ノート、トレーニング ビデオ、ラボおよび Cisco Live セッション、ソーシャル メディア チャ

ネル、Cisco ブログおよび技術文書チームによって公開されたすべてのドキュメンテーションへのリンクが含まれます。

管理人等、コミュニティサイトや動画共有サイトに情報を掲載する個人が、シスコの社員であることがあります。それらのサイトおよび対応するコメントで表明される意見は、投稿者本人の個人的意見であり、シスコの意見ではありません。掲載内容は、情報の提供のみを目的としており、シスコや他の関係者による推奨または異議を目的としたものではありません。

（注） ファイアウォール コミュニティ の動画、テクニカル ノート、および参考資料の中には、古いバージョンの Firepower Management Center に言及しているものがあります。ご使用のバージョンの Firepower Management Center と動画やテクニカル ノートで参照されているバージョンとではユーザ インターフェイスに違いがあるために、手順も異なる場合があります。