Firepower の概要

Cisco Firepowerは、専用プラットフォームで展開されるか、ソフトウェア ソリューションとして展開される、ネットワーク セキュリティおよびトラフィック管理製品の統合スイートです。このシステムは、組織のセキュリティ ポリシー（ネットワークを保護するためのガイドライン）に準拠する方法でネットワーク トラフィックを処理できるように設計されています。

標準的な展開では、ネットワーク セグメントにインストールされた複数のトラフィック検知管理対象デバイスが分析対象のトラフィックをモニタし、マネージャにレポートします。

- Firepower Management Center
- Firepower Device Manager
- Adaptive Security Device Manager（ASDM）

マネージャでは、集中管理コンソールのグラフィカル ユーザ インターフェイスを使用して管理、分析、およびレポート タスクを実行できます。

このガイドでは、*Firepower Management Center* 管理アプライアンスについて説明します。ASDMを介して管理される Firepower Device Manager または ASA with FirePOWER Services については、これらの管理手法のガイドを参照してください。

- *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager*
- *ASA with FirePOWER Services Local Management Configuration Guide*

クイック スタート：基本設定

Firepower の機能セットには、基本設定および詳細設定をサポートできるだけの強力さと柔軟性があります。以降に説明する手順に従って、Firepower Management Center とその管理対象デバイスを迅速に設定し、トラフィックの制御と分析を開始することができます。

物理アプライアンスでの初期セットアップのインストールと実行

手順

目的のアプライアンスに対応するドキュメンテーションを使用して、すべての物理アプライアンスで初期セットアップをインストールおよび実行します。

- **Firepower Management Center**
  - ハードウェア モデルについては、『*Cisco Firepower Management Center Getting Started Guide*』を参照してください。次のサイトから入手できます。

    http://www.cisco.com/go/firepower-mc-install

- **Firepower Threat Defense 管理対象デバイス**

  重要　次のページの Firepower Device Manager ドキュメントは無視してください。

  - ISA 3000 対応の Firepower Threat Defense：『*Cisco Firepower Threat Defense for the ISA 3000 Using Firepower Management Center Quick Start Guide*』

    http://www.cisco.com/go/ftd-quick
  - 2100 対応の Firepower Threat Defense：『*Cisco Firepower Threat Defense for the Firepower 2100 Series Using Firepower Management Center Quick Start Guide*』

    http://www.cisco.com/go/ftd-quick
  - 4100 対応の Firepower Threat Defense：『*Cisco Firepower Threat Defense for Firepower 4100 Quick Start Guide*』

    http://www.cisco.com/go/ftd-quick
  - 9300 対応の Firepower Threat Defense：『*Cisco Firepower Threat Defense for Firepower 9300 Quick Start Guide*』

    http://www.cisco.com/go/ftd-quick
  - ASA 5508-X/5516-X 対応の Firepower Threat Defense：『*Cisco Firepower Threat Defense for the ASA 5508-X and ASA 5516-X Using Firepower Management Center Quick Start Guide*』

    http://www.cisco.com/go/ftd-quick

- ASA 5500-X 対応の Firepower Threat Defense：『*Cisco Firepower Threat Defense for the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X Using Firepower Management Center Quick Start Guide*』

  http://www.cisco.com/go/ftd-quick

- ASA 5506-X 対応の Firepower Threat Defense：『*Cisco Firepower Threat Defense for the ASA 5506-X Series Using Firepower Management Center Quick Start Guide*』

  http://www.cisco.com/go/ftd-quick

- **従来型管理対象デバイス**

  - ASA FirePOWER サービス管理対象デバイス：『*Cisco ASA FirePOWER Module Quick Start Guide*』

    http://www.cisco.com/go/asafp-quick

  - 8000 シリーズ管理対象デバイス：『*Cisco Firepower 8000 Series Getting Started Guide*』

    http://www.cisco.com/go/8000series-install

  - 7000 シリーズ管理対象デバイス：『*Cisco Firepower 7000 Series Getting Started Guide*』

    http://www.cisco.com/go/7000series-install

仮想アプライアンスの展開

展開に仮想アプライアンスが含まれている場合は、以下の手順に従います。ドキュメンテーション ロードマップを使用して、http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html にリストされているドキュメントを見つけます。

手順

ステップ 1 Management Center とデバイスで使用する、サポートされている仮想プラットフォームを決定します（これらは同一とは限りません）。詳細については、『*Cisco Firepower Compatibility Guide*』を参照してください。

ステップ 2 ご使用の環境に応じたドキュメンテーションを使用して、仮想 Firepower Management Center を展開します。

- VMware で実行されている Firepower Management Center Virtual：『*Cisco Firepower Management Center Virtual for VMware Deployment Quick Start Guide*』
- AWS で実行されている Firepower Management Center Virtual：『*Cisco Firepower Management Center Virtual for AWS Deployment Quick Start Guide*』
- KVM で実行されている Firepower Management Center Virtual：『*Cisco Firepower Management Center Virtual for KVM Deployment Quick Start Guide*』

ステップ 3 ご使用のアプライアンスに応じたドキュメンテーションを使用して、仮想デバイスを展開します。

- VMware で実行されている NGIPSv：『*Cisco Firepower NGIPSv Quick Start Guide for VMware*』
- VMware で実行されている Firepower Threat Defense Virtual：『*Cisco Firepower Threat Defense for the ASA 5508-X and ASA 5516-X Using Firepower Management Center Quick Start Guide*』
- AWS で実行されている Firepower Threat Defense Virtual：『*Cisco Firepower Threat Defense Virtual for AWS Deployment Quick Start Guide*』
- KVM で実行されている Firepower Threat Defense Virtual：『*Cisco Firepower Threat Defense Virtual for KVM Deployment Quick Start Guide*』
- Azure で実行されている Firepower Threat Defense Virtual：『*Cisco Firepower Threat Defense Virtual for Azure Deployment Quick Start Guide*』

最初のログイン

始める前に

- アプライアンスを準備します。詳細については、物理アプライアンスでの初期セットアップのインストールと実行 （2 ページ）または仮想アプライアンスの展開 （3 ページ）を参照してください。

手順

ステップ 1 ユーザ名として **admin**、パスワードとして **Admin123** を使用して、Firepower Management Center の Web インターフェイスにログインします。このアカウントのパスワードは、ご使用のアプライアンスの『クイック スタート ガイド』の説明に従って変更してください。

ステップ 2 このアカウントのタイム ゾーンを設定します。詳細については、デフォルト タイム ゾーンの設定を参照してください。

ステップ 3 ライセンスを追加します。詳細については、Firepower システムのライセンスを参照してください。

ステップ 4 管理対象デバイスを登録します。詳細については、Firepower Management Center へのデバイスの追加を参照してください。

ステップ 5 管理対象デバイスを設定します。手順については、次を参照してください。

- IPS デバイスの展開と設定の概要7000 シリーズまたは 8000 シリーズのデバイスで、パッシブ インターフェイスまたはインライン インターフェイスを設定する場合。
- Firepower Threat Defense インターフェイスについてFirepower Threat Defense デバイスで、トランスペアレント モードまたはルーテッド モードを設定する場合。

- Firepower Threat Defense インターフェイスについてFirepower Threat Defense デバイスで、インターフェイスを設定する場合。

次のタスク

- 基本ポリシーを設定することで、トラフィックの制御と分析を開始します。詳細については、基本ポリシーの設定 （5 ページ）を参照してください。

基本ポリシーの設定

ダッシュボード、コンテキスト エクスプローラ、およびイベント テーブルにデータを表示するには、基本ポリシーを設定し、展開する必要があります。

（注） これはポリシーや機能に関する完全な説明ではありません。その他の機能とより高度な設定については、このガイドの他のセクションを参照してください。

始める前に

- 最初のログイン （4 ページ）の説明に従って、Web インターフェイスにログインして、タイム ゾーンを設定し、ライセンスを追加し、デバイスを登録し、デバイスを設定します。

手順

ステップ 1 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って、アクセス コントロール ポリシーを設定します。

- ほとんどの場合、デフォルトのアクションとして、セキュリティと接続のバランスの取れた侵入ポリシーを設定することが提案されます。詳細については、アクセス コントロール ポリシーのデフォルト アクションおよびシステム提供のネットワーク分析ポリシーと侵入ポリシーを参照してください。
- ほとんどの場合、組織のセキュリティとコンプライアンスのニーズを満たすために接続のロギングを有効にすることが提案されます。表示を整理したり、システムに負担をかけないために、ログに記録する接続を決定する際はネットワークのトラフィックを考慮してください。詳細については、接続ロギングについてを参照してください。

ステップ 2 正常性ポリシーの適用の説明に従って、システムが提供するデフォルトの正常性ポリシーを適用します。

ステップ 3 いくつかのシステム設定をカスタマイズします。

- サービス（SNMP や syslog など）の受信接続を許可する場合は、システムのアクセス リストの設定の説明に従ってアクセス リストのポートを変更します。
- データベース イベント数の制限の設定の説明に従って、データベース イベント制限の編集について理解し、検討します。
- 表示言語を変更する場合は、別の言語の指定の説明に従って言語設定を編集します。
- 組織がプロキシ サーバを使用してネットワーク アクセスを制限しており、初期設定時にプロキシを設定しなかった場合は、Firepower Management Center 管理インターフェイスの設定の説明に従ってプロキシ設定を編集します。

ステップ 4 ネットワーク検出ポリシーの設定の説明に従って、ネットワーク検出ポリシーをカスタマイズします。デフォルトでは、ネットワーク検出ポリシーは、ネットワークのすべてのトラフィックを分析します。ほとんどの場合、RFC 1918 のアドレスに検出を制限することが提案されます。

ステップ 5 次の他の一般的な設定のカスタマイズを検討します。

- メッセージセンターのポップアップを表示しない場合は、通知動作の設定の説明に従って通知を無効にします。
- システム変数のデフォルト値をカスタマイズする場合は、変数セットの説明に従ってそれらの用途を理解します。
- 地理位置情報データベースを更新する場合は、地理位置情報データベース（GeoDB）の更新の説明に従って手動またはスケジュールに基づいて更新します。
- アプライアンスにアクセスする追加のローカル認証ユーザ アカウントを作成する場合は、社内ユーザ アカウントの追加を参照してください。
- LDAP または RADIUS 外部認証を使用してアプライアンスへのアクセスを許可する場合は、外部認証の設定を参照してください。

ステップ 6 設定変更を展開します。設定変更の展開を参照してください。

次のタスク

- Firepower システム機能 （8 ページ）およびこのガイドの他のセクションに記載されているその他の機能の設定について確認し、検討してください。

Firepower デバイス

標準的な展開では、ネットワーク セグメントにインストールされた複数のトラフィック処理デバイスは、トラフィックを分析して、物理または仮想 Firepower Management Center のいずれかにレポートします。Firepower Management Center では、集中管理コンソールのグラフィカル ユーザ インターフェイスを使用して管理、分析、およびレポート タスクを実行できます。

この項では、トラフィック処理デバイスにインストールして Firepower Management Center で管理できる Firepower の実装について説明します。

特定のデバイス モデル、仮想ホスティング環境、オペレーティング システムなどと互換性のあるソフトウェアを含むマネージャとデバイスの互換性の詳細については、次のドキュメントロードマップで入手できる『*Cisco Firepower Compatibility Guide*』を参照してください。
http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html

Firepower Threat Defense（NGFW）

物理プラットフォームまたは仮想プラットフォーム上で統合された次世代ファイアウォール（NGFW）および次世代 IPS（NGIPS）デバイスを提供する軽量ソフトウェア。Firepower ソフトウェアのモデルで使用可能な NGIPS 機能に加えて、NGFW およびプラットフォーム機能には、サイト間およびリモート アクセス VPN、堅牢なルーティング、NAT、クラスタリング、およびアプリケーションインスペクションとアクセス制御におけるその他の最適化が含まれています。

Firepower ソフトウェア（NGIPS）

7000 および 8000 シリーズ Firepower デバイス上で稼働するか、または VMware 上でホストされる NGIPS ソフトウェア。

ASA with FirePOWER サービス（NGIPS）

ASA デバイス上で稼働する NGIPS ソフトウェア。ASA デバイスは、第 1 のシステム ポリシーを提供し、トラフィックを ASA FirePOWER モジュールに渡し検出およびアクセス制御を行います。

ASA FirePOWER には ASA プラットフォームに固有のソフトウェアとコマンドライン インターフェイス（CLI）があります。ASA 専用のこれらのツールを使用して、システムのインストールおよびプラットフォーム固有のその他の管理タスクを実行します。

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、デバイス高可用性、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。
- インターフェイス設定：Firepower Management Center の Web インターフェイスを使用して ASA FirePOWER のインターフェイスを設定することはできません。Firepower Management Center では、ASA FirePOWER が SPAN ポート モードで展開されている場合、ASA インターフェイスを表示しません。
- 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。

Firepower システム機能

次の表では、Firepower システムで最も一般に設定される機能について説明します。次に示す未知のドキュメントを見つけるには、ドキュメンテーション ロードマップを使用します。http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html。

表 *1*：一般に設定される *Firepower* システム機能

目的	設定	参照先
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	アクセス制御の概要
IP アドレス、URL、またはドメイン名との間でブラックリストまたはホワイトリスト接続する	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 インテリジェンスについて
ネットワークのユーザがアクセスできる Web サイトを制御する	ポリシー ルール内の URL フィルタリング	URL 条件（URL フィルタリング）
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	侵入ポリシーの基本
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	SSL ポリシーの概要
ディープ インスペクションをカプセル化トラフィックに合わせて調整し、高速パス処理でのパフォーマンスを向上させる	プレフィルタ ポリシー	プレフィルタの概要
アクセス コントロールによって許可または信頼されたネットワーク トラフィックのレート制限	サービス品質（QoS）ポリシー	QoS ポリシーについて
ネットワーク上のファイル（マルウェアを含む）を許可またはブロックする	ファイル ポリシー	ファイル ポリシー
脅威インテリジェンス ソースからデータを運用可能にします。	Cisco Threat Intelligence Director（TID）	Cisco Threat Intelligence Director（TID） の概要

目的	設定	参照先
継続的なファイル分析のためにパブリックまたはプライベート クラウドに照会する	パブリック AMP クラウドまたは AMP プライベート クラウド（AMPv）への接続	AMP クラウド接続
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	ユーザ アイデンティティ ソースについて ユーザ アイデンティティ ソースについて アイデンティティ ポリシーについて
ユーザ認識を実行するために、ネットワークのトラフィックからホスト、アプリケーション、およびユーザ データを収集する	ネットワーク検出ポリシー	概要：ネットワーク検出ポリシー
アプリケーション検出およびコントロールを実行する	アプリケーション ディテクタ	概要：アプリケーション検出
アプライアンスへのログイン用のユーザ アカウントを制御する	内部または外部認証（あるいはその両方）	ユーザ アカウントについて
システム ハードウェアとシステム ソフトウェアの状況をモニタする	ヘルス モニタリング ポリシー	ヘルス モニタリングについて
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概要
システムを Firepower システムの新しいバージョンに更新する	システムの更新	FirePOWER ソフトウェアのアップグレード *Firepower System Release Notes*
物理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への復元（再イメージ化）	*Cisco Firepower Management Center Getting Started Guide* *Cisco Firepower 7000 Series Getting Started Guide* *Cisco Firepower 8000 Series Getting Started Guide* *Reimage the Cisco ASA or Firepower Threat Defense Device*

目的	設定	参照先
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	脆弱性データベースの更新 侵入ルールの更新 地理位置情報データベース（GeoDB）の更新
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	クラシック ライセンスまたはスマート ライセンス	Firepower の機能ライセンスについて
アプライアンスの動作の継続性を確保する	管理対象デバイスの高可用性または Firepower Management Center の高可用性（あるいはその両方）	7000 および 8000 シリーズ デバイスのハイ アベイラビリティについて ハイ アベイラビリティ Firepower Threat Defense について Firepower Management Center のハイ アベイラビリティについて
複数の 8000 シリーズのデバイスの処理リソースを結合する	デバイス スタッキング	デバイス スタックについて
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	仮想ルータ Firepower Threat Defense のルーティングの概要
複数のネットワーク間のパケットスイッチングを設定する	デバイス スイッチング	仮想スイッチ のブリッジグループ インターフェイスの設定
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）	NAT ポリシーの設定 Firepower Threat Defense 用のネットワーク アドレス変換（NAT）
管理対象の Firepower Threat Defense または 7000/8000 シリーズ デバイス間のセキュアなトンネルを確立する	サイト間バーチャル プライベート ネットワーク（VPN）	VPN の概要
リモート ユーザと管理対象 Firepower Threat Defense デバイス間のセキュアなトンネルを確立する	リモート アクセス VPN	VPN の概要

目的	設定	参照先
管理対象デバイス、設定、およびイベントへのユーザ アクセスをセグメント化する	ドメインを使用したマルチテナンシー	ドメインを使用したマルチテナンシーの概要
REST API クライアントを使用してアプライアンスの設定を表示および管理する	REST API および REST API エクスプローラ	REST API 設定 *Firepower REST API Quick Start Guide*
Firepower Management Center から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 データをストリームする	eStreamer 統合	eStreamer サーバ ストリーミング *Firepower System eStreamer Integration Guide*
サードパーティ クライアントを使用して Firepower Management Center のデータベース テーブルを照会する	外部データベース アクセス	外部データベース アクセスの設定 *Firepower System Database Access Guide*
サードパーティ ソースからデータをインポートすることによって検出データを増やす	ホスト入力	ホスト入力データ *Firepower System Host Input API Guide*
ネットワークの条件が、関連付けられたポリシーに違反した場合、自動的に修復を起動する	修復	修復の概要 *Firepower System Remediation API Guide*

アプライアンスごとのハイアベイラビリティ、クラスタリング、およびスタック構成機能

以下で説明するように、ハイ アベイラビリティ構成、クラスタ化構成、およびスタック構成で FirePOWER アプライアンスを展開できます。

（フェールオーバーとも呼ばれる）ハイ アベイラビリティ構成により、操作の継続性が確保されます。クラスタ化構成とスタック構成では、複数のデバイスが単一の論理デバイスとしてグループ化され、スループットと冗長性が向上します。

アプライアンス	高可用性	クラスタリング	スタック構成
Firepower Management Center	Yes	No	No
Firepower Management Center Virtual	No	No	No

アプライアンス	高可用性	クラスタリング	スタック構成
以下で稼働している Firepower NGIPS Firepower 7010、7020、7030、7050 Firepower 7110、7115、7120、7125、AMP7150 Firepower 8120、8130、AMP8050、AMP8150	Yes	No	No
以下で稼働している Firepower NGIPS Firepower 8140 Firepower 8250、8260、8270、8290 Firepower 8350、8360、8370、8390、AMP8350	Yes	No	Yes
以下で稼働している Firepower Threat Defense 仮想：VMware 仮想：KVM	Yes	No	No
以下で稼働している Firepower Threat Defense パブリック クラウド：AWS パブリック クラウド：Azure	No	No	No
以下で稼働している Firepower Threat Defense ASA5506-X、06H-X、06W-X、08-X、16-X ASA5512-X、15-X、25-X、45-X、55-X	Yes	No	No
以下で稼働している Firepower Threat Defense Firepower 9300	Yes	Yes	No
以下で稼働している Firepower Threat Defense Firepower 4110、4120、4140、4150	Yes	Yes	No
以下で稼働している Firepower Threat Defense Firepower 2110、2120、2130、2140	Yes	No	No

関連トピック

7000 および 8000 シリーズ デバイスのハイ アベイラビリティについて
ハイ アベイラビリティ Firepower Threat Defense について
Firepower Management Center のハイ アベイラビリティについて

Firepower のオンライン ヘルプとドキュメンテーション

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。
- **[ヘルプ（Help）] > [オンライン（Online）]** を選択する。

ドキュメンテーション ロードマップを使用して、Firepowerに関連する追加ドキュメンテーションを見つけることができます（http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html）。

Firepower Management Center 展開に関するトップレベルのドキュメントのリスト ページ

Firepower Management Center 展開のバージョン 6.0+ を設定するときは、次のドキュメントが役立つ可能性があります。

（注） リンクされたドキュメントの一部は、Firepower Management Center 展開には適用できません。たとえば、Firepower Threat Defense ページの一部のリンクは Firepower Device Manager によって管理される展開に固有の内容で、ハードウェア ページの一部のリンクは FirePOWER とは無関係です。混乱を避けるために、ドキュメントのタイトルには十分に注意してください。また、一部のドキュメントは複数の製品を対象としているため、複数の製品のページに記載されていることがあります。

Firepower Management Center

- Firepower Management Center ハードウェア アプライアンス：

  http://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html

- Firepower Management Center Virtual アプライアンス：
  - http://www.cisco.com/c/en/us/support/security/defense-center-virtual-appliance/tsd-products-support-series-home.html
  - http://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html

NGFW（次世代ファイアウォール）デバイスとも呼ばれる Firepower Threat Defense

- Firepower Threat Defense ソフトウェア：

  http://www.cisco.com/c/en/us/support/security/firepower-ngfw/tsd-products-support-series-home.html

- Firepower Threat Defense Virtual：

http://www.cisco.com/c/en/us/support/security/firepower-ngfw-virtual/tsd-products-support-series-home.html

- FirePOWER 2100 シリーズ：

  https://www.cisco.com/c/en/us/support/security/firepower-2100-series/tsd-products-support-series-home.html

- FirePOWER 4100 シリーズ：

  https://www.cisco.com/c/en/us/support/security/firepower-4100-series/tsd-products-support-series-home.html

- FirePOWER 9300：

  https://www.cisco.com/c/en/us/support/security/firepower-9000-series/tsd-products-support-series-home.html

- ASA 5500-X シリーズ：
  - 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

- ISA 3000 ハードウェア：

  https://www.cisco.com/c/en/us/support/security/industrial-security-appliance-isa/tsd-products-support-series-home.html

NGIPS（次世代侵入防御システム）デバイスとも呼ばれる従来型デバイス

- ASA with FirePOWER Services：
  - ASA 5500-X with FirePOWER Services：
    - 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

- FirePOWER 8000 シリーズ：

  https://www.cisco.com/c/en/us/support/security/firepower-8000-series-appliances/tsd-products-support-series-home.html

- FirePOWER 7000 シリーズ：

  https://www.cisco.com/c/en/us/support/security/firepower-7000-series-appliances/tsd-products-support-series-home.html

- AMP for Networks：

  https://www.cisco.com/c/en/us/support/security/amp-appliances/tsd-products-support-series-home.html

- NGIPSv（バーチャル デバイス）：

  https://www.cisco.com/c/en/us/support/security/ngips-virtual-appliance/tsd-products-support-series-home.html

ドキュメンテーションのライセンス ステートメント

項の先頭に記載されているライセンス ステートメントは、項で説明される機能を有効にするために Firepower システムの管理対象デバイスに割り当てる必要があるのは従来のライセンスかスマート ライセンスかを示します。

ライセンス付きの機能の多くは追加的であるため、ライセンス ステートメントでは、各機能で最も必要なライセンスについてのみ記載しています。

ライセンス文の「または」という語は、その項に記載されている機能を有効にするには特定のライセンスを管理対象デバイスに指定する必要があることを示していますが、追加のライセンスで機能を追加できます。たとえば、ファイル ポリシー内では、一部のファイル ルール アクションではデバイスに保護ライセンスを指定する必要がありますが、他方ではマルウェア ライセンスを指定する必要があります。

ライセンスの詳細については、Firepower の機能ライセンスについてを参照してください。

関連トピック

Firepower の機能ライセンスについて

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、スタッキングは 8000 シリーズ のデバイスでのみ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。事前定義のロールを使用して、ある手順に対するアクセス要件を示す場合は、類似の権限を持つカスタム ロールもアクセス権限を持っています。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を付与されたカスタム 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。

ユーザ ロールの詳細については、ユーザの役割およびWeb インターフェイス用のユーザ ロールのカスタマイズを参照してください。

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

この詳細なドキュメントの補足として、次の動画や参考資料をご利用いただけます。

（注） このセクションにリンクされている動画、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 を指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。

- 教育およびトレーニング （17 ページ）
- ソーシャル メディア チャネル （17 ページ）
- 設定例 （17 ページ）
- トラブルシューティング （17 ページ）

メモ 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。本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。

教育およびトレーニング

- Next-Generation Firewall Resource Center：シスコの次世代ファイアウォールについて知る必要があるすべてを学習できるリソースです。
- 『Cisco Firepower Threat Defense (FTD) Common Practices Guide』：実際の顧客のインストール環境から導出された、Cisco FTD の展開におけるポリシーおよびデバイス管理に関する推奨事項と一般的な慣習が記載されたインタラクティブなマニュアルです。
- 『Configuration and Troubleshooting Best Practices for the Next-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), and Advanced Malware Protection (AMP)』（著者：Nazmul Rajib、ISBN：9781587144806）：シスコのグローバル テクニカル サポート センター（TAC）では、このビジュアル ガイドを参照して、Cisco Firepower の次世代セキュリティ テクノロジーに関する実践的で詳細な情報を得ることを強く推奨しています。

ソーシャル メディア チャネル

- 専門家や IT プロフェッショナルからなるシスコのコミュニティで、シスコの次世代ファイアウォールに関する質問の答えを得ることができます。シスコのコミュニティ ページは年中無休です。このページにアクセスして専門知識が集まるコミュニティを利用することにより、専門家とネットワークで繋がって、投資の最適化に役立つ機会が得られます。
- シスコの YouTube チャネルに登録して、当社のテクニカル マーケティング エンジニアやテクニカル アシスタンス センター（TAC）が作成したビデオをご覧ください。
  - Cisco Advanced Security の管理
  - Cisco Firepower Threat Defense を使用したネットワーク保護
  - シスコのセキュリティ TME
  - Jason Maynard
- セキュリティ関連の最新情報を概観するには、シスコのブログにご登録ください。

設定例

シスコのテクニカル サポート エンジニアは、複雑な Firepower シナリオを取得する構成ユースケースとテクニカル ノートを作成します。これらは必要に応じて更新されます。

トラブルシューティング

テクニカル ノートは、最も複雑ないくつかの問題を解決するためのガイダンスを提供しています。お使いの製品の製品ドキュメント ページの「Troubleshoot and Alerts」という見出しの下にある、テクニカル ノートとその他のトラブルシューティング リソースを探します。これらの

ページのリストについては、Firepower Management Center 展開に関するトップレベルのドキュメントのリスト ページ （13 ページ）を参照してください。