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。

  - sco Firepower 2100 Series Getting Started Guide
  - Cisco Firepower 4100 Getting Started Guide
  - Cisco Firepower 9300 Getting Started Guide
  - Cisco Firepower Threat Defense for the ASA 5508-X and ASA 5516-X Using Firepower Management Center Quick Start Guide
  - 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
  - Cisco Firepower Threat Defense for the ISA 3000 Using Firepower Management Center Quick Start Guide

- **従来型管理対象デバイス**
  - Cisco ASA FirePOWER Module Quick Start Guide
  - Cisco Firepower 8000 Series Getting Started Guide
  - Cisco Firepower 7000 Series Getting Started Guide

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『*Quick Start Guide*』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 のインターフェイスの概要：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 のインターフェイスの概要：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 （4 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、「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、「Web インターフェイスの言語の設定」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 機能 （7 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

一般的な展開では、複数のトラフィック処理デバイスが、アドミニストレーション、管理、分析、および報告タスクの実行に使用される 1 つの Firepower Management Center に報告します。

従来のデバイス

従来のデバイスは、次世代 IPS（NGIPS）ソフトウェアを実行します。具体的には以下のとおりです。

- Firepower 7000 シリーズおよび Firepower 8000 シリーズの物理デバイス。
- VMware でホストされている NGIPSv。
- ASA with FirePOWER Services は、一部の ASA 5500-X シリーズ デバイス（ISA 3000 も含む）で使用できます。ASA 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 デバイスで ASA ベースの機能を設定するには、ASA CLI または ASDM を使用する必要があります。これには、デバイスのハイ アベイラビリティ、スイッチング、ルーティング、VPN、NAT などが含まれます。FMC 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。また、ASA FirePOWER が SPAN ポートモードで展開されている場合、FMC GUI は ASA インターフェイスを表示しません。また、FMC を使用して ASA FirePOWER プロセスのシャットダウン、再起動、またはその他の管理を行うことはできません。

Firepower Threat Defense デバイス

Firepower Threat Defense（FTD）デバイスは、NGIPS 機能も備えた次世代ファイアウォール（NGFW）です。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。

FTD は、幅広い物理プラットフォームおよび仮想プラットフォームで使用できます。

互換

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、『Cisco Firepower Release Notes』および『Cisco Firepower Compatibility Guide』を参照してください。

Firepower 機能

次の表には、一般的に使用されるいくつかの Firepower 機能が一覧表示されています。

アプライアンスおよびシステム管理の機能

未知のドキュメントを検索するには、http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html を参照してください。

目的	設定	参照先
Firepower アプライアンスへのログイン用のユーザ アカウントを管理する	Firepower 認証	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
新しい Firepower バージョンにアップグレードする	システムの更新プログラム	Cisco Firepower Management Center Upgrade Guide Firepower Release Notes

目的	設定	参照先
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に復元（再イメージ化）する	Cisco Firepower Management Center Upgrade Guide、新規インストールの実行に関する説明へのリンクの一覧。
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	システム ソフトウェアの更新
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	従来のライセンスまたはスマート ライセンス	Firepower 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 デバイスまたは 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）	Firepower Threat Defense の VPN の概要

目的	設定	参照先
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	Firepower Threat Defense の VPN の概要
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*
問題のトラブルシューティング	該当なし	システムのトラブルシューティング

プラットフォーム別のハイ アベイラビリティとスケーラビリティの機能

（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。

プラットフォーム	高可用性	クラスタリング	スタック構成
Firepower Management Center	あり MC750 を除く	—	—
Firepower Management Center Virtual	—	—	—
Firepower Threat Defense： • • Firepower 2100 シリーズ • ASA 5500-X シリーズ • ISA 3000	あり	—	—
Firepower Threat Defense： • Firepower 4100/9300 シャーシ	あり	あり	—
Firepower Threat Defense Virtual： • VMware • KVM	あり	—	—

プラットフォーム	高可用性	クラスタリング	スタック構成
Firepower Threat Defense Virtual（パブリック クラウド）： • AWS • Azure	—	—	—
• Firepower 7010、7020、7030、7050 • Firepower 7110、7115、7120、7125 • Firepower 8120、8130 • AMP 7150、8050、8150	あり	—	—
• Firepower 8140 • Firepower 8250、8260、8270、8290 • Firepower 8350、8360、8370、8390 • AMP 8350	あり	—	Yes
ASA FirePOWER	—	—	—
NGIPSv	—	—	—

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

潜在的な脅威を検出、防御、および処理するための機能

未知のドキュメントを検索するには、http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html を参照してください。

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

目的	設定	参照先
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 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（Intrusion Policy）	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	プレフィルタリングについて
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/マルウェア ポリシー	ファイル ポリシーと高度なマルウェア防御
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
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 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
外部ツールを使用してネットワーク トラフィックと潜在的な脅威に関するデータを収集して分析する	外部ツールとの統合	外部ツールを使用したイベントの分析
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

目的	設定	参照先
問題のトラブルシューティング	該当なし	システムのトラブルシューティング

外部ツールとの統合

未知のドキュメントを検索するには、http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html を参照してください。

目的	設定	参照先
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*
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*
外部イベント データ ストレージ ツールその他のデータ リソースを使用してイベントを調査します。	外部イベント分析ツールとの統合	外部ツールを使用したイベントの分析
問題のトラブルシューティング	該当なし	システムのトラブルシューティング

Firepower Management Center のドメインの切り替え

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
該当なし	任意	FMC	任意	任意

マルチドメイン導入環境では、ユーザ ロール権限によって、ユーザがアクセスできるドメインと、そのドメイン内でのユーザの権限が決まります。単一のユーザアカウントを複数のドメインに関連付けて、各ドメインでそのユーザに異なる権限を割り当てることができます。たとえば、あるユーザにグローバル ドメインでは読み取り専用権限を割り当て、子孫ドメインでは管理者権限を割り当てることができます。

複数のドメインに関連付けられているユーザは、同じ Web インターフェイス セッション内でドメインを切り替えることができます。

ツールバーのユーザ名の下に、利用可能なドメインのツリーが表示されます。ツリーの表示は次のようになります。

- 先祖ドメインは表示されますが、使用しているユーザアカウントに割り当てられた権限に応じて、先祖ドメインへのアクセスが無効である場合があります。
- 兄弟ドメインや子孫ドメインを含め、使用しているユーザアカウントでアクセスできない他のドメインは非表示になります。

ドメインを切り替えると、以下の項目が表示されます。

- そのドメインのみに関連するデータ。
- そのドメインで割り当てられたユーザ ロールに応じて定められたメニュー オプション。

手順

アクセスするドメインは、ユーザ名の下にあるドロップダウン リストから選択します。

コンテキスト メニュー

Firepower システム Web インターフェイスの特定のページでは、右クリック（最も一般的）および左クリックでコンテキスト メニューを表示できます。コンテキスト メニューは、Firepower システム内の他の機能にアクセスするためのショートカットとして使用できます。コンテキスト メニューの内容はどこでこのメニューにアクセスするか（どのページかだけでなく特定のデータにアクセスしているか）によって異なります。

次に例を示します。

- IP アドレスのホットスポットでは、そのアドレスに関連付けられているホストに関する情報（使用可能な whois とホスト プロファイル情報を含む）が表示されます。
- SHA-256 ハッシュ値のホットスポットでは、ファイルの SHA-256 ハッシュ値をクリーン リストまたはカスタム検出リストに追加したり、コピーするためにハッシュ値全体を表示したりできます。

Firepower システム コンテキスト メニューをサポートしていないページや場所では、ブラウザの通常のコンテキスト メニューが表示されます。

ポリシー エディタ

多くのポリシーエディタには、各ルールのホットスポットが含まれています。新しいルールとカテゴリの挿入、ルールの切り取り、コピー、貼り付け、ルール状態の設定、ルールの編集などを行うことができます。

侵入ルール エディタ

侵入ルールエディタには、各侵入ルールのホットスポットが含まれています。ルールの編集、ルール状態の設定、しきい値および抑止オプションの設定、ルールのドキュメンテーションの表示などを行うことができます。必要に応じて、コンテキストメニューで、**ルールのドキュメント**をクリックするより具体的なルールの詳細を表示するドキュメントのポップアップ ウィンドウで、**ルールのドキュメント**をクリックすることができます。

イベント ビューア

イベントページ（[分析（Analysis）]ページにあるドリルダウンページとテーブル ビュー）には、各イベント、IP アドレス、URL、DNS クエリ、特定のファイルの SHA-256 ハッシュ値のホットスポットが含まれています。ほとんどのイベント タイプでは、表示中に以下の操作を行うことができます。

- Context Explorer で関連情報を表示する。
- 新しいウィンドウでイベント情報をドリルダウンする。
- イベント フィールドに含まれているテキスト（ファイルの SHA-256 ハッシュ値、脆弱性の説明、URL など）が長すぎてイベント ビューですべて表示できない場合、テキスト全体を表示する。
- コンテキスト クロス起動機能を使用し、Firepower の外部のソースからのエレメントに関する情報が表示されている Web ブラウザ ウィンドウを開きます。詳細については、「Web ベースのリソースを使用したイベントの調査」を参照してください。
- （組織で Cisco Security Packet Analyzer が展開されている場合）イベントに関連するパケットを調べます。詳細については、「Cisco Security Packet Analyzerを使用したイベント調査」を参照してください。

接続イベントの表示中は、デフォルトのセキュリティ インテリジェンスのホワイトリストとブラックリストに以下の項目を追加できます。

- IP アドレスのホットスポットの場合、IP アドレス。
- URL のホットスポットの場合、URL またはドメイン名。
- DNS クエリのホットスポットの場合、DNS クエリ。

キャプチャ ファイル、ファイル イベント、マルウェア イベントの表示中は、以下の操作を行うことができます。

- クリーン リストまたはカスタム検出リストのファイルを追加または削除する。

- ファイルのコピーをダウンロードする。
- アーカイブ ファイル内のネストされたファイルを表示する。
- ネストされたファイルの親アーカイブ ファイルをダウンロードする。
- ファイルの構成を表示する。
- ローカル マルウェア分析およびダイナミック分析対象のファイルを送信する。

侵入イベントの表示中は、侵入ルールエディタまたは侵入ポリシーで実行できるようなタスクを行うことができます。

- トリガー ルールを編集する。
- ルールの無効化を含め、ルールの状態を設定する。
- しきい値および抑止オプションを設定する。
- ルールのドキュメンテーションを表示する。必要に応じて、コンテキスト メニューの [ルール ドキュメント（Rule documentation）] をクリックした後、ドキュメント ポップアップ ウィンドウの [ルール ドキュメント（Rule Documentation）] をクリックするとより具体的なルールの詳細情報を表示できます。

侵入イベントのパケット ビュー

侵入イベントのパケット ビューには、IP アドレスのホットスポットが含まれています。パケット ビューでは、左クリックによるコンテキスト メニューを使用します。

ダッシュボード

多くのダッシュボード ウィジェットには、関連する情報を Context Explorer で表示するためのホットスポットが含まれています。ダッシュボード ウィジェットには、IP アドレスと SHA-256 ハッシュ値のホットスポットが含まれる場合もあります。

Context Explorer

Context Explorer には、図、表、グラフのホットスポットが含まれています。Context Explorer よりも詳細なグラフまたはリストのデータを調べたい場合は、関連するデータのテーブル ビューにドリルダウンすることができます。また、関連するホスト、ユーザ、アプリケーション、ファイル、および侵入ルールの情報を表示できます。

Context Explorer でも左クリックのコンテキスト メニューを使用します。これには、Context Explorer に特有のフィルタリングおよび他のオプションも含まれています。

関連トピック

セキュリティ インテリジェンスのリストとフィード

シスコとのデータの共有

次の機能を使用して、シスコとデータを共有することを選択できます。

- Cisco Success Network

  「Cisco Success Network」を参照してください

- Web 分析

  「（オプション）Web 分析トラッキングのオプトアウト」を参照してください

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。
- **[ヘルプ（Help）]** > **[オンライン（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 [ハウツー（How To）] ウィジェットは有効になっています。このウィジェットを無効にするには、自分のユーザ名の下にあるドロップダウン リストから [ユーザ設定（User Preferences）] を選択し、[ハウツーの設定（How-To Settings）] タブの [ハウツーを有効にする（Enable How-Tos）] 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。

FMC 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：

  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

- ISA 3000 with FirePOWER Services：

  https://www.cisco.com/c/en/us/support/security/industrial-security-appliance-isa/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 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 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、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。

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

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。

関連リソース