Management Center の概要

このガイドは、プライマリマネージャまたは分析専用マネージャとしてのオンプレミスの Secure Firewall Management Center に適用されます。Cisco Security Cloud Control（Security Cloud Control）クラウド提供型 Firewall Management Center をプライマリマネージャとして使用する場合、オンプレミスの Firewall Management Center は分析のみに使用できます。Security Cloud Control の管理にはこのガイドを使用しないでください。「Cisco Security Cloud Control のクラウド提供型 Firewall Management Center を使用した Firewall Threat Defense の管理」を参照してください。

Secure Firewall Management Center は強力な Web ベースのマルチデバイスマネージャです。独自のサーバーハードウェア上で、またはハイパーバイザ上の仮想デバイスとして稼働します。マルチデバイスマネージャを必要とし、Firewall Threat Defense のすべての機能が必要な場合は、Firewall Management Center を使用する必要があります。Firewall Management Center は、トラフィックとイベントの強力な分析とモニタリングも提供します。

（注） Security Cloud Control 管理対象デバイスがあり、オンプレミス Firewall Management Center を分析のみに使用している場合、オンプレミス Firewall Management Center はポリシーの設定またはアップグレードをサポートしません。このガイドの一部の章と手順は、プライマリマネージャが Security Cloud Control であるデバイスには適用されない可能性があります。

Firewall Management Center をプライマリマネージャとして使用する場合：Firewall Management Center は独自の Firewall Threat Defense 設定があり、Firewall Management Center をバイパスして Firewall Threat Defense を直接設定できないため、Firewall Management Center は他のマネージャと互換性がありません。

クイック スタート：基本設定

Cisco Secure Firewall 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、Secure Firewall 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。

- **Firewall Management Center**
  - ハードウェアモデルについては、『Cisco Secure 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。

    『Cisco Secure Firewall Management Center Getting Started Guides』
- **Firewall Threat Defense 管理対象デバイス**
  - Cisco Firepower 1010 スタートアップガイド
  - Cisco Firepower 1100 Getting Started Guide
  - Cisco Secure Firewall 3100 Getting Started Guide
  - Cisco Firepower 4100 スタートアップガイド
  - Cisco Secure Firewall 4200 スタートアップガイド
  - Cisco Firepower 9300 スタートアップ ガイド
  - 『Cisco Secure Firewall Threat Defense for the ISA 3000 Using Secure Firewall Management Center Quick Start 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、次のドキュメントを見つけてください：『Navigating the Cisco Secure Firewall Threat Defense Documentation』

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）。『*Cisco Secure Firewall 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 Cisco Secure Firewall Management Center を展開します。

- VMware で実行されている Firewall Management Center Virtual：『*Cisco Secure Firewall Management Center Virtual Getting Started Guide*』
- AWS で実行されている Firewall Management Center Virtual：『*Cisco Secure Firewall Management Center Virtual Getting Started Guide*』
- KVM で実行されている Firewall Management Center Virtual：『*Cisco Secure Firewall Management Center Virtual Getting Started 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 Firewall Threat Defense Virtual：『*Cisco Secure Firewall Threat Defense Virtual for VMware Getting Started Guide*』
- AWS で実行されている Firewall Threat Defense Virtual：『*Cisco Secure Firewall Threat Defense Virtual for AWS Getting Started Guide*』
- KVM で実行されている Firewall Threat Defense Virtual：『*Cisco Secure Firewall Threat Defense Virtual for KVM Getting Started Guide*』
- Azure で実行されている Firewall Threat Defense Virtual：『*Cisco Secure Firewall Threat Defense Virtual for Azure Getting Started Guide*』

最初のログイン

新しい Firewall Management Center に初めてログインする前に、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）の説明に従ってアプライアンスを準備します。

新しい Firewall Management Center（または工場出荷時の初期状態に新しく復元された Firewall Management Center）に初めてログインするときは、CLI または Web インターフェイスの **admin** アカウントを使用して、お客様の Firewall Management Center モデル用の『*Cisco Cisco Secure Firewall Management Center Getting Started Guide*』の手順に従ってください。初期設定プロセスが完了したら、システムの次の側面を設定します。

- 2 つの **admin** アカウント（1 つは Web インターフェイスアクセス用、もう 1 つは CLI アクセス用）のパスワードは、Firewall Management Center のユーザーアカウントの注意事項と制約事項で説明されている強力なパスワード要件に準拠した同じ値に設定されます。システムは、最初の設定プロセス中にのみ 2 つの **admin** アカウントのパスワードを同期します。その後、いずれかの **admin** アカウントのパスワードを変更すると、パスワードは同じではなくなり、Web インターフェイスの **admin** アカウントから強力なパスワード要件を削除できます。（内部ユーザーの追加または編集を参照）。
- Firewall Management Center が管理インターフェイス（eth0）を介したネットワーク通信に使用する次のネットワーク設定は、デフォルト値または指定した値に設定されます。
  - 完全修飾ドメイン名（`<hostname>.<domain>`）
  - IPv4 設定用のブートプロトコル（DHCP またはスタティック/手動）
  - IPv4 アドレス
  - ネットワーク マスク
  - ゲートウェイ
  - DNS サーバー
  - NTP サーバー

  これらの設定値は、Firewall Management Center Web インターフェイスを使用して表示および変更できます。詳細については、Firewall Management Center 管理インターフェイスの変更および時刻の同期を参照してください。
- Cisco Success Network 機能と Cisco Support Diagnostic 機能は、デフォルトで有効になっています。シスコは、Cisco Secure Firewall デバイスからテレメトリデータを収集し、カスタマー サクセス イニシアチブに使用します。シスコによって収集されるテレメトリデータの詳細については、『Cisco Success Network Telemetry Data Collected from the Management Center Devices』を参照してください。
- アップグレードまたは新規インストール後に**管理者**権限を持つユーザーが Firewall Management Center に初めてログインすると、**管理者**ユーザーに電子メールアドレスの入力を求める 1 回限りのプロンプトが表示されます。電子メールアドレスの入力は任意です。シスコでは、商談や製品更新の案内、新しいリリースの導入に関するニュースレターの提供、その他の製品関連通信の共有を目的として、電子メールアドレスを収集し、使用しています。
- 初期構成の一環として、システムは週次 GeoDB 更新をスケジュールします。このタスクを確認し、必要に応じ、GeoDB 更新のスケジューリング。

- 初期構成の一環として、システムは週ごとのダウンロードをスケジュールします。このタスクを確認し、必要に応じ、ソフトウェア ダウンロードの自動化。

重要 このタスクは、更新のみをダウンロードします。ユーザは、このタスクがダウンロードした更新をインストールする必要があります。

- 初期構成の一環として、システムは（ローカルに保存された）設定のみの週次 Firewall Management Center バックアップをスケジュールします。このタスクを確認し、必要に応じ、Firewall Management Center のバックアップのスケジュール。
- 初期構成の一環として、システムは最新の VDB をダウンロードしてインストールします。システムを最新の状態に保つために、「 脆弱性データベースの更新の自動化。
- 初期構成の一環として、システムは日次の侵入ルール更新をスケジュールします。このタスクを確認し、必要に応じ、侵入ルールの更新のスケジュール。

Firewall Management Center の初期設定が完了すると、Web インターフェイスには、Cisco Secure Firewall Management Center デバイス構成ガイドで説明されている [デバイス管理（Device Management）] ページが表示されます

（このページは、**admin** ユーザーが初めてログインしたときにのみ使用されるデフォルトのログイン ページです。**admin** またはユーザーによる以降のログインでは、ホームページの指定の説明に従ってデフォルトのログイン ページが決定されます）。

初期設定を完了したら、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

Web インターフェイスまたは CLI の **admin** アカウントを使用して Web インターフェイスにログインし、ご使用のハードウェアモデル用の『*Cisco Cisco Secure Firewall Management Center Getting Started Guide*』（[インストールおよびアップグレードガイド（Install and Upgrade Guides）]https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-guides-list.htmlから取得できます）の説明に従って初期設定を行います。

手順

ステップ 1 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 2 必要に応じて、ライセンスの説明に従ってライセンスを追加します。

ステップ 3 Cisco Secure Firewall Management Center デバイス構成ガイドの「*Add a Device to the Firewall Management Center*」の説明に従って、管理対象デバイスを展開に追加します。

ステップ 4 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。

- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Interface Overview*」：Firewall 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。
- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Interface Overview*」：Firewall Threat Defense デバイスのインターフェイスを設定する場合。

ステップ 5 Cisco Secure Firewall Management Center デバイス構成ガイドの「*Creating a Basic Access Control Policy*」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（Cisco Secure Firewall Management Center デバイス構成ガイド）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 6 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 7 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ーを使用してネットワークアクセスを制限している場合は、Firewall Management Center 管理インターフェイスの変更の説明に従ってプロキシ設定を編集します。

ステップ 8 Cisco Secure Firewall Management Center デバイス構成ガイドの「*Configuring the Network Discovery Policy*」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 9 次の他の一般的な設定のカスタマイズを検討します。

- 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、Cisco Secure Firewall Management Center デバイス構成ガイドの「*Variable Sets*」の説明に従ってそれらの用途を理解します。
- Firewall Management Center にアクセスする追加のローカル認証ユーザーアカウントを作成する場合は、内部ユーザーの追加または編集を参照してください。
- LDAP または RADIUS 外部認証を使用して Firewall Management Center へのアクセスを許可する場合は、Firewall Management Center の外部認証の設定を参照してください。

ステップ 10 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

次のタスク

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。

最新バージョンのデバイスでサポートされていない画面

Firewall Management Center は、以前のバージョン（Cisco Secure Firewall Threat Defense 互換性ガイドで入手可能な互換性マトリックスで指定されています）を実行しているデバイスを管理できますが、このガイドには、最新バージョンのデバイスソフトウェアでサポートされている機能のみが含まれています。

古いバージョンのデバイスでのみサポートされている機能については、ご使用のバージョンに一致するガイドを参照してください。

最新バージョンのデバイスでサポートされていない Snort 2 画面

画面が Snort 2 機能用であるため、このヘルプ ページにリダイレクトされました。Snort 2 は、Threat Defense バージョン 7.7 以降ではサポートされていません。7.7 より前のバージョンでサポートされている Snort 2 機能については、ご使用の Firewall Threat Defense のバージョンに対応する Firewall Management Center のガイドを参照してください。

Firewall Threat Defense 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 Secure Firewall Management Center に報告します。

Firewall Threat Defense 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。

Firewall Threat Defense 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。

互換性

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 Secure Firewall Threat Defense リリースノート、Cisco Secure Firewall Management Center 互換性ガイド、および Cisco Secure Firewall Threat Defense 互換性ガイドを参照してください。

機能

次の表には、一般的に使用されるいくつかの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

ドキュメントを検索するには、Cisco Secure Firewall Threat Defense ドキュメントにアクセスを参照してください。

目的	設定	参照先
Cisco Secure Firewall デバイスへのログイン用のユーザーアカウントを管理する	デバイス認証	Firewall Management Center ユーザー および Cisco Secure Firewall Management Center デバイス構成ガイドの「*Users for Devices*」
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ーする	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/復元

目的	設定	参照先
新しい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	Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド Cisco Secure Firewall Threat Defense リリースノート
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 FXOS トラブルシューティング ガイド（Threat Defense を実行している Firepower 1000/2100 および Cisco Secure Firewall 1200/3100/4200 向け）
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
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	スマートライセンシング	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 Firewall Management Center の高可用性（あるいはその両方）	Cisco Secure Firewall Management Center デバイス構成ガイドの「*About Cisco Secure Firewall Threat Defense "High Availability chapter"*」 Firewall Management Center のハイ アベイラビリティについて
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	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Reference for Routing*」
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	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Configure Bridge Group Interfaces*」
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 Secure Firewall Management Center デバイス構成ガイドの「*Network Address Translation*」

目的	設定	参照先
管理対象の Firewall Threat Defense 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）	Cisco Secure Firewall Management Center デバイス構成ガイドの「*VPN Overview*」
リモートユーザーと管理対象 Firewall 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	Cisco Secure Firewall Management Center デバイス構成ガイドの「*VPN Overview*」
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 『*Cisco Secure Firewall Mangement Center REST API Quick Start Guide*』
問題のトラブルシューティング	N/A	トラブルシューティング

潜在的な脅威を検出、防御、および処理するための機能

ドキュメントを検索するには、Cisco Secure Firewall Threat Defense ドキュメントにアクセス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	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Introduction to Access Control*」
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またはモニターする	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	Cisco Secure Firewall Management Center デバイス構成ガイドの「*About Security Intelligence*」
ネットワークのユーザーがアクセスできる 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	Cisco Secure Firewall Management Center デバイス構成ガイドの「*URL Filtering*」

目的	設定	参照先
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	Cisco Secure Firewall Management Center デバイス構成ガイドの*Snort 3* 侵入ポリシーの開始
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	Cisco Secure Firewall Management Center デバイス構成ガイドの「*SSL Policies Overview*」
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	Cisco Secure Firewall Management Center デバイス構成ガイドの「*About Prefiltering*」
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	Cisco Secure Firewall Management Center デバイス構成ガイドの「*About QoS Policies*」
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	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Network Malware Protection and File Policies*」
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 Secure Firewall Management Center デバイス構成ガイドの「*Secure Firewall Threat Intelligence Director Overview*」
ユーザーの認知およびユーザー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ー認証を設定する	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	Cisco Secure Firewall Management Center デバイス構成ガイドの「*About User Identity Sources*」 Cisco Secure Firewall Management Center デバイス構成ガイドの「*About Identity Policies*」

目的	設定	参照先
ユーザー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、およびユーザー データを収集する	ネットワーク検出ポリシー	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Network Discovery Policies*」
デバイス外の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	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Application Detection*」
問題のトラブルシューティング	N/A	トラブルシューティング

外部ツールとの統合

ドキュメントを検索するには、Cisco Secure Firewall Threat Defense ドキュメントにアクセス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*』
Firewall 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 サーバー ストリーミング 『*Cisco Secure Firewall Mangement Center Event Streamer Integration Guide*』
サードパーティクライアントを使用して Firewall 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 『*Cisco Secure Firewall Mangement Center Database Access Guide*』

目的	設定	参照先
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	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Host Input Data*」 『*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	N/A	トラブルシューティング

Firewall Management Center を検索します。

グローバル検索機能を使用して、Secure Firewall Management Center 設定の要素をすばやく見つけて移動することができます。

次のエンティティの Firewall Management Center 設定を検索できます。

- トップレベルメニューの Web インターフェイスページの名前。（Web インターフェイス メニューのオプションの検索 （16 ページ） を参照。）
- 特定のポリシータイプについて：
  - ポリシー名
  - ポリシーの説明
  - ルール名
  - ルールのコメント

  （ポリシーの検索 （17 ページ） を参照。）
- 特定のオブジェクトタイプについて：
  - オブジェクト名
  - オブジェクトの説明
  - 設定値

  （オブジェクトの検索 （19 ページ）を参照）。
- How To ウォークスルー。

  検索すると、検索語を含むウォークスルーのリストと、各ウォークスルーへのリンクが返されます。（How To ウォークスルーの検索 （24 ページ） を参照。）

グローバル検索を使用するときは、次のことに注意してください。

- グローバル検索ツールを開くと、検索テキストボックスの下の履歴リストに、最近の 10 件の検索が表示されます。このリストから項目を選択して、検索を再実行できます。
- 検索式を入力すると、インターフェイスの検索履歴が検索結果に置き換わり、検索を入力するにつれて更新されます。検索を実行するために Enter キーを押す必要はありません。
- マウスまたはキーボードの矢印キーと Enter キーを使用して、履歴リストまたは検索結果を移動できます。Enter キーを押すと、検索結果で現在強調表示されている項目が選択されます。Web インターフェイスページの結果の場合は、強調表示されたページが Firewall Management Center インターフェイスに表示されます。オブジェクトとポリシーの場合は、見つかったエンティティに関する詳細が表示されます。
- 検索では大文字と小文字が区別されません。
- 検索では、次のワイルドカード文字を使用できます。
  - ? は、任意の単一文字と一致します。
  - * は、0 文字以上の任意の文字と一致します。
  - ^ は、前にある検索用語を一致するエンティティの先頭に固定します。
  - $ は、後ろにある検索用語を一致するエンティティの末尾に固定します

  ワイルドカードはエスケープできません。
- 効率を高めるために、グローバル検索では間接的な検索結果は返されません。つまり、検索用語が見つかったオブジェクトを参照するポリシーやオブジェクトは返されません。ただし、検索の詳細ペインで見つかったオブジェクトの [使用状況（Usages）] タブを表示することで、多くの見つかったオブジェクトを参照しているポリシーまたはオブジェクトを判断することができます。
- グローバル検索では、Firewall Management Center で最も一般的に使用される設定エンティティとの関連性によって決定される、検索式の上位の結果が返されます。グローバル検索で期待していた結果が返されなかった場合は、検索を絞り込むか、多くの GUI ページの上部に表示される検索ツールまたはフィルタツールを使用するか、Web インターフェイスによって提供されている設定固有の検索機能を試してみてください。
  - Cisco Secure Firewall Management Center デバイス構成ガイド のルールの検索
  - Cisco Secure Firewall Management Center デバイス構成ガイド の *NAT* ルールテーブルの検索とフィルタリング
  - イベントの検索
  - カスタム テーブルの検索

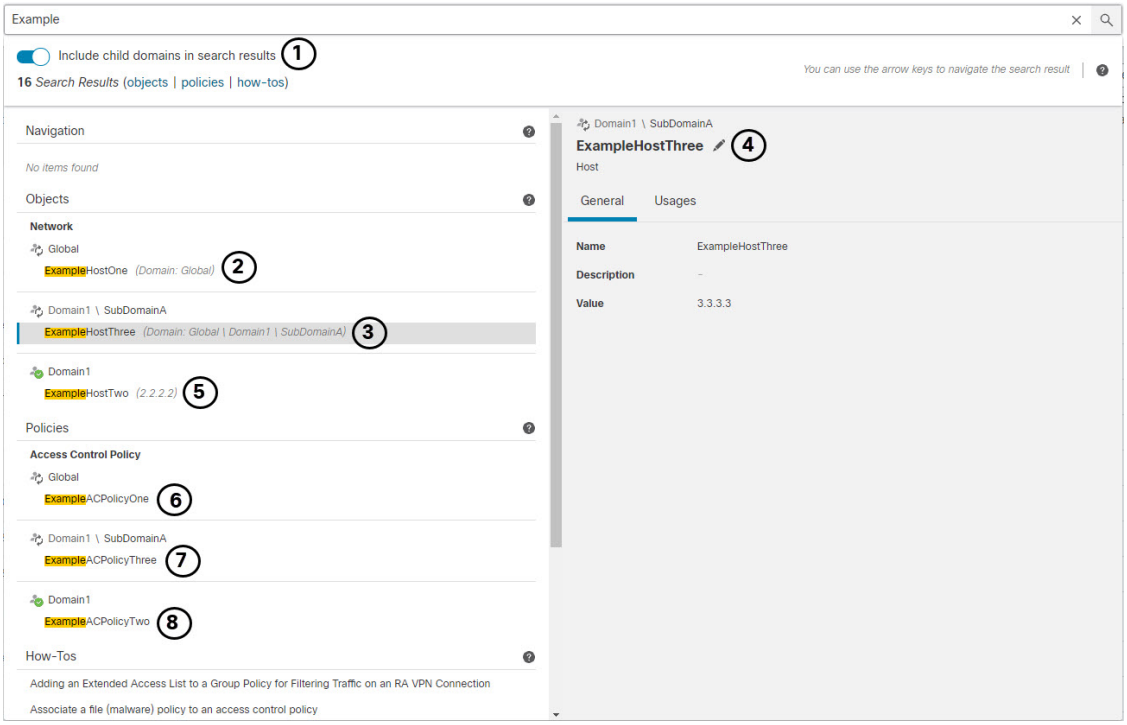
マルチドメイン展開でのグローバル検索

マルチドメイン展開の検索では、現在のドメインとその先祖ドメイン内で定義されているオブジェクトとポリシーのみがデフォルトで返されます。検索結果ダイアログのオプションを切り替えることで、子ドメインのオブジェクトとポリシーを表示できます。

オブジェクト検索では、現在のドメイン以外のドメインで定義されたオブジェクトで検索式が見つかった場合、検索結果には、それらのオブジェクトが存在するドメインの名前が表示されます。現在のドメイン内で定義されたオブジェクトで検索式が見つかった場合、検索結果にはオブジェクトの値が表示されます。

次のスクリーンショットの例では、展開は、Global、Domain1、および SubDomainA の 3 つのレベルのドメインで構成されています。現在のドメインが Domain1 であるユーザーが、先祖ドメインと子ドメインの両方で文字列「example」の検索を入力しました。

図 *1*: マルチドメイン環境でのグローバル検索の例



1	ユーザーは、子ドメイン（SubDomainA）、現在のドメイン（Domain1）、およびその先祖（Global）を検索することを選択しました。	2	親ドメイン Global で定義された一致するネットワークオブジェクト ExampleHostOne がドメイン名とともに表示されます。[外部ドメイン（External Domain）]（） アイコンは、詳細を編集するためにはドメインを切り替える必要があることを示しています。

3	子ドメイン SubDomainA で定義された一致するネットワークオブジェクト ExampleHostThree がドメイン名とともに表示されます。[外部ドメイン（External Domain）]（）アイコンは、詳細を編集するためにはドメインを切り替える必要があることを示しています。このオブジェクトは現在選択されています。	4	一致するネットワークオブジェクト ExampleHostThree が現在選択されており、右側のペインに情報が表示されています。[外部ドメイン（External Domain）]（  ）アイコンは、[編集（Edit）]（  ）をクリックしたときに、オブジェクトへの編集アクセスを許可する前にドメインの変更を確認するためのユーザープロンプトが表示されることを示しています。
5	現在のドメインで定義されている一致するネットワークオブジェクト ExampleHostTwo がオブジェクト値とともに表示されます。[現在のドメイン（Current Domain）]（）アイコンは、ドメインを切り替えずにこのオブジェクトを編集できることを示しています。	6	親ドメイン Global で定義された一致するアクセス コントロール ポリシー ExampleACPolicyOne がドメイン名とともに表示されます。[外部ドメイン（External Domain）]（）アイコンは、詳細を編集するためにドメインを切り替える必要があることを示しています。
7	子ドメイン SubDomainA で定義された一致するアクセス コントロール ポリシー ExampleACPolicyThree がドメイン名とともに表示されます。[外部ドメイン（External Domain）]（）アイコンは、詳細を編集するためにドメインを切り替える必要があることを示しています。	8	現在のドメインで定義されている一致するアクセス コントロール ポリシー ExampleACPolicyTwo が [現在のドメイン（Current Domain）]（  ）アイコンとともに表示されます。このアイコンは、ドメインを切り替えずに詳細を編集できることを示しています。

Web インターフェイスメニューのオプションの検索

Webインターフェイスのトップレベルメニューで、ページの場所を検索して見つけることができます。たとえば、Quality of Service の設定を表示または構成するには、**QoS** を検索します。

手順

ステップ 1 検索を開始するには、次の 2 つの方法のいずれかを使用します。

- Firewall Management Center Web インターフェイスの上部にあるメニューバーで、[検索（Search）]（  ）をクリックします。
- テキストボックスの外側にフォーカスを置いて、/（スラッシュ）を入力します。

ステップ 2 探しているメニューオプションの名前を 1 文字以上入力します。検索結果がテキストボックスの下に表示され、入力すると更新されます。検索を実行するために Enter キーを押す必要はありません。

ステップ 3 検索結果はカテゴリ別にグループ化されて表示されます。[ナビゲーション（Navigation）] の下に表示されたページに移動するには、検索結果リストのメニューパスをクリックします。

ポリシーの検索

次の表は、名前で検索できるポリシータイプを示しています。

範囲内	範囲外
アクセス コントロール ポリシー（Access Control Policy）	Threat Defense プラットフォーム設定
プレフィルタポリシー（Prefilter Policy）	Firepower 設定ポリシー
Threat Defense NAT ポリシー	Firepower NAT ポリシー
侵入カテゴリ • 侵入ポリシー（Intrusion Policy） • ネットワーク分析ポリシー（Network Analysis Policy）	QoS ポリシー（QoS Policy） FlexConfig ポリシー（FlexConfig Policy） DNS ポリシー マルウェア & ファイル ポリシー SSL ポリシー（SSL Policy） ID ポリシー ネットワーク検出 アプリケーションディテクタ 相関ポリシー VPN カテゴリ • ダイナミック アクセス ポリシー • サイト間 • リモートアクセス

グローバル検索では、名前が検索語句に一致するポリシーと、名前またはコメントが検索語句に一致するルールが使用されているアクセス コントロール ポリシーが返されます。名前が検索内容に一致しないアクセス コントロール ポリシーが検索結果リストに表示された場合は、ポリシー内で設定されているルールの名前またはコメントが一致しています。

重要 グローバル検索では、Firewall Management Center で最も一般的に使用される設定エンティティとの関連性によって決定される、検索式の上位の結果が返されます。この検索機能の範囲外のポリシータイプに検索語句が含まれている可能性があります。グローバル検索機能と代替検索方法の詳細については、「Firewall Management Center の検索」を参照してください。

手順

ステップ 1 検索を開始するには、次の 2 つの方法のいずれかを使用します。

- Firewall Management Center Web インターフェイスの上部にあるメニューバーで、[検索（Search）] （） をクリックします。
- テキストボックスの外側にフォーカスを置いて、/（スラッシュ）を入力します。

ステップ 2 検索テキストボックスに検索式を入力します。検索結果がテキストボックスの下に表示され、入力すると更新されます。検索を実行するために Enter キーを押す必要はありません。

ステップ 3 （オプション）マルチドメイン展開では、現在のドメインに子孫ドメインがある場合、[検索結果に子ドメインを含める（Include child domains in search results）] を切り替えて、子孫ドメイン内のポリシーを表示できます。

ステップ 4 検索結果はカテゴリ別にグループ化されて表示されます。マルチドメイン展開では、[ポリシー（Policies）] カテゴリ内で、検出されたポリシーが定義されているドメインによって検索結果がグループ化されます。[ポリシー（Policies）] カテゴリでは、次のことができます。

方法：	操作手順
単一ポリシータイプの検索結果を表示します。	検索結果で、アクセスコントロールポリシーなどのポリシータイプをクリックします。
ポリシーに関する詳細を表示します。	検索結果リストのポリシー名をクリックして詳細ペインを表示し、[全般（General）] タブを表示します。
侵入ポリシーとネットワーク分析ポリシーを参照するアクセスコントロールポリシーを表示します。	検索結果の侵入ポリシーまたはネットワーク分析ポリシーの名前をクリックして詳細ペインを表示し、[使用状況（Usages）] タブを表示します。

方法：	操作手順
別のブラウザウィンドウでポリシーのポリシー設定ページを開きます。	検索結果でポリシー名をクリックし、詳細ペインで [編集（Edit）]（） をクリックします。 マルチドメイン展開では、現在のドメイン内で定義されていないポリシーを編集することを選択すると、現在のドメインの変更を求められます。

オブジェクトの検索

次の表は、[オブジェクト管理（Object Management）] ページ（**[オブジェクト（Objects）]**>**[オブジェクト管理（Object Management）]**）に一覧表示されるオブジェクトタイプのうち、グローバル検索機能の範囲内にあるものを示しています。

範囲内	範囲外
AAA サーバーカテゴリ • RADIUS サーバー グループ • シングルサインオンサーバー アクセスリストカテゴリ • 拡張アクセス リスト • 標準アクセス リスト アドレスプールカテゴリ • IPv4 プール • IPv6 プール AS パス（AS Path） コミュニティリストカテゴリ • 拡張コミュニティ DNS サーバ グループ 外部属性カテゴリ • ダイナミックオブジェクト • セキュリティグループタグ 位置情報 インターフェイスカテゴリ • セキュリティ ゾーン • インターフェイス グループ	アプリケーション フィルタ 暗号スイート リスト コミュニティリストカテゴリ • コミュニティ（Community） 識別名カテゴリ • 個々の識別名オブジェクト • 識別名オブジェクトグループ ファイル リスト FlexConfig カテゴリ • FlexConfig オブジェクト • テキストオブジェクト PKI カテゴリ • 外部証明書グループ（External Cert Groups） • 外部証明書 • 内部 CA グループ（Internal CA Groups） • 内部 CA • 内部証明書グループ（Internal Cert Groups） • 内部証明書 • 信頼できる CA グループ（Trusted CA Groups） • 信頼できる CA

範囲内	範囲外
キーチェーン ネットワーク（ネットワーク、ホスト、範囲、FQDN、ネットワークグループを含む） PKI カテゴリ 証明書の登録 ポリシー リスト ポート（オブジェクトとグループ、TCP、UDP、ICMP、ICMP6、その他） プレフィックス リスト カテゴリ • IPv4 プレフィックス リスト • IPv6 プレフィックス リスト ルートマップ SLA モニタ 時間範囲 タイムゾーン トンネル ゾーン URL（オブジェクト、グループ） VLAN タグ（オブジェクト、グループ） VPN カテゴリ • 証明書マップ • [グループ ポリシー（Group Policy）] • IKEv1 IPSec プロポーザル • IKEv1 ポリシー • IKEv2 IPSec プロポーザル • IKEv2 ポリシー	セキュリティ インテリジェンス カテゴリ • DNS リストとフィード • ネットワークリストとフィード • [URLのリストとフィード（URL Lists and Feeds）] シンクホール 変数セット VPN カテゴリ • Secure Client ファイル • カスタム属性

グローバル検索では、名前または説明が検索用語に一致するオブジェクトと、検索用語に一致する構成値を持つオブジェクトが返されます。名前が検索内容に一致しないオブジェクトが検索結果リストに表示された場合は、オブジェクト内の説明または構成値が一致しています。

重要 グローバル検索では、Firewall Management Center で最も一般的に使用される設定エンティティとの関連性によって決定される、検索式の上位の結果が返されます。この検索機能の範囲外のオブジェクトタイプに検索用語が含まれている可能性があります。グローバル検索機能と代替検索方法の詳細については、「Firewall Management Center の検索」を参照してください。

オブジェクト検索は、展開内のネットワーク情報を見つける必要がある場合に特に役立ちます。オブジェクト名、説明、または構成値で次のものを検索できます。

- 次の形式を含む、IPv4 および IPv6 アドレス情報。
  - 完全なアドレス（たとえば、`194.164.0.23`、`2001:0db8:85a3:0000:0000:8a2e:0370:7334`）。
  - 部分的なアドレス（たとえば、`194.164`、`2001:db8`）。
  - 範囲（たとえば、`192.164.1.1-192.168.1.5`、`2001:db8::0202-2001:db8::8329`。ハイフンの前後にスペースを入力しないでください。）グローバル検索は、指定された範囲内のいずれかに一致するネットワークアドレスを使用してオブジェクトを返します。
  - CIDR 表記。（たとえば、`192.168.1.0/24`、`2002::1234:abcd:ffff:101/64`。）グローバル検索は、指定された CIDR ブロック内のいずれかに一致するネットワークアドレスを使用してオブジェクトを返します。
- ポート情報：
  - ポート番号（たとえば、`22` または `80`）。
  - プロトコル。（たとえば、`https` または `ssh`。）
- 完全修飾ドメイン名。（たとえば、`www.cisco.com`）
- URL。（たとえば、`http://www.cisco.com`）
- 暗号化標準規格またはハッシュタイプ（たとえば、`AES-128` または `SHA`）。
- VLAN タグ番号（たとえば、`568`）。

手順

ステップ 1 検索を開始するには、次の 2 つの方法のいずれかを使用します。

- Firewall Management Center Web インターフェイスの上部にあるメニューバーで、[検索（Search）]（  ）をクリックします。

- テキストボックスの外側にフォーカスを置いて、/（スラッシュ）を入力します。

ステップ 2 検索テキストボックスに検索式を入力します。検索結果がテキストボックスの下に表示され、入力すると更新されます。検索を実行するために Enter キーを押す必要はありません。

現在のデフォルトドメイン以外のドメインで定義されたオブジェクトで検索式が見つかった場合、検索結果には、それらのオブジェクトが存在するドメインの名前が表示されます。現在のドメイン内で定義されたオブジェクトで検索式が見つかった場合、検索結果にはオブジェクトの値が表示されます。

ステップ 3 （オプション）マルチドメイン展開では、現在のドメインに子孫ドメインがある場合、[検索結果に子ドメインを含める（Include child domains in search results）] を切り替えて、子孫ドメイン内のオブジェクトを表示できます。

ステップ 4 検索結果はカテゴリ別に分けて表示されます。マルチドメイン展開では、[オブジェクト（Objects）] カテゴリ内で、検出されたオブジェクトが定義されているドメインによって検索結果がグループ化されます。[オブジェクト（Objects）] カテゴリでは、次のことができます。

方法：	操作手順
単一オブジェクトタイプの検索結果を表示します。	検索結果で、[ネットワーク（Network）] などのオブジェクトタイプをクリックします。
検索結果のオブジェクトに関する詳細を表示します。	検索結果のオブジェクト名をクリックして詳細ペインを表示し、[全般（General）] タブを表示します。
検索結果のオブジェクトを使用するポリシーまたはオブジェクトのリストを表示します。	検索結果のオブジェクト名をクリックして詳細ペインを表示し、[使用状況（Usages）] タブを表示します。 （注） グローバル検索では、すべてのオブジェクトタイプの使用情報を得られるわけではありません。
オブジェクトのオブジェクト設定ページを別のブラウザウィンドウで開きます。	検索結果でオブジェクト名をクリックし、詳細ペインで [編集（Edit）]（）をクリックします。 マルチドメイン展開では、現在のドメイン内で定義されていないオブジェクトを編集することを選択すると、現在のドメインの変更を求められます。

How To ウォークスルーの検索

関心のあるタスクに対処する How To ウォークスルーを検索できます。たとえば、デバイスのセットアップ手順が説明されているウォークスルーを検索するには、「device」という用語を検索します。

始める前に

この機能は、クラシックテーマでは使用できません。テーマを変更するには、Web インターフェイス表示の変更を参照してください。

手順

ステップ 1 検索を開始するには、次の 2 つの方法のいずれかを使用します。

- Firewall Management Center Web インターフェイスの上部にあるメニューバーで、[検索（Search）]（  ）をクリックします。
- テキストボックスの外側にフォーカスを置いて、/（スラッシュ）を入力します。

ステップ 2 ウォークスルーを表示するタスクに関連付けられた検索用語を入力します。検索結果がテキストボックスの下に表示され、入力すると更新されます。検索を実行するために Enter キーを押す必要はありません。

ステップ 3 検索結果はカテゴリ別にグループ化されて表示されます。[How-Tos] にリストされているウォークスルーを表示するには、検索結果リストでウォークスルーのタイトルをクリックします。How To ウォークスルーの詳細については、オンラインヘルプ、How To、 およびドキュメント（27 ページ）を参照してください。

Secure Firewall Management Center のドメインの切り替え

マルチドメイン導入環境では、ユーザー ロール権限によって、ユーザー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ー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、ユーザー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**をクリックした後、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。

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ブロックリストとブロックしない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。

シスコとのデータの共有

Cisco Success Network 機能と Cisco Support Diagnostic 機能は、デフォルトで有効になっています。

シスコでは、Cisco Success Network の機能を通じて、シスコ製品のカスタマーエクスペリエンスを向上させるために、お客様の使用状況のメトリックと統計情報を収集しています。シスコへの Cisco Success Network テレメトリデータの送信をオプトアウトするには、使用状況のメトリックと統計をシスコと共有するための Firewall Management Center の設定を参照してください。シスコによって収集されるテレメトリデータの詳細については、『Cisco Success Network Telemetry Data Collected from the Management Center Devices』を参照してください。

Cisco Support Diagnostics の機能を通じて、シスコはお客様のデバイスから重要な情報を収集し、充実したサポートエクスペリエンスをお届けしています。シスコへの Cisco Support Diagnostics メトリックの送信をオプトアウトするには、デバイス正常性データをシスコと共有するための Firewall Management Center の設定を参照してください。

Web分析を使用して、シスコとデータを共有することを選択できます。詳細については、「Web分析」を参照してください。

オンラインヘルプ、How To、 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）]** > **[ページレベルのヘルプ（Page-level Help）]** を選択する。

How To は、Firewall 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。[How To] ウィジェットはデフォルトで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。[How To] ウィジェットを開くには、**[ヘルプ（Help）]** > **[How-Tos]**を選択します。

（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、ユーザーの権限によっては Firewall Management Center 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。

Firewall Management Center では、次のウォークスルーを利用できます。

Firewall Management Center でサポートされている機能ウォークスルーのリストについては、「Feature Walkthroughs Supported in Secure Firewall Management Center」を参照してください。

ドキュメンテーション ロードマップを使用して、その他のドキュメントを検索できます。

Cisco Secure Firewall Threat Defense ドキュメントにアクセス。

cisco.com のユーザーガイド

Secure Firewall 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、Secure Firewall Management Center 展開には適用できません。たとえば、Secure Firewall Threat Defense ページの一部のリンクは Secure Firewall 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 Firewall Management Center 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。

Secure Firewall Management Center

- Secure Firewall 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

- Secure Firewall 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 Secure Firewall Threat Defense

- Secure Firewall 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

- Secure Firewall Threat Defense Virtual：

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

- FirePOWER 1000 シリーズ：

  https://www.cisco.com/c/en/us/support/security/firepower-1000-series/tsd-products-support-series-home.html

- Secure Firewall 3100：

  https://www.cisco.com/c/en/us/support/security/secure-firewall-3100-series/series.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

- Secure Firewall 4200：

  https://www.cisco.com/c/en/us/support/security/secure-firewall-4200-series/series.html

- FirePOWER 9300：

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

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防御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、「ライセンスについて」を参照してください。

関連トピック

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 Secure Firewall 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Firewall 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 Firewall 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ー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

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。