システム設定

この章では、Secure Firewall Management Center でのシステム構成設定方法について説明します。

Firewall Management Center と Cisco Security Cloud] の統合

Cisco Security Cloud は、ファイアウォールの導入を広範なシスコの統合型セキュリティ クラウドサービスにつなげ、可視性を統合し、自動化を可能にし、ネットワーク、エンドポイント、アプリケーション全体のセキュリティを強化する一貫した体験を提供します。Cisco Security Cloud が提供するシンプルで、より統合されたクラウドサービスを使用するプラットフォームアプローチで、複数の製品を管理する複雑性を軽減できます。

Cisco Security Cloud Control アカウントを使用して、Firewall Management Center を Cisco Security Cloud で承認し、登録します。この統合により、ファイアウォールの展開が Cisco Cloud テナントに導入準備され、次のような機能が提供されます。

- 複数の Firewall Management Center に一貫したポリシーを確立します。
- Firewall Threat Defense デバイスの ゼロ タッチ プロビジョニング を実装します。
- クラウドにイベントを送信し、さまざまな Cisco Security Cloud サービスを使用して、脅威ハンティングと調査を強化します。
- Firewall Management Center 全体のインベントリの一元化されたビューを取得する

Firewall Management Center の Security Cloud Control への導入準備の詳細については、オンプレミス Management Center の導入準備を参照してください。

Secure Firewall Management Center と Cisco XDR を統合するには、『Cisco Secure Firewall Management Center と Cisco XDR の統合ガイド』を参照してください。

Cisco Security Cloud 統合の有効化

Firewall Management Center と Cisco Security Cloud を統合して、Firewall Management Center とその管理対象デバイスの両方を Security Cloud Control テナントにオンボードします。Firewall Management Center が Security Cloud Control に対してオンボードされると、その管理対象デバイスの表示、管理対象ネットワークオブジェクトの表示、および Firewall Management Center UI への相互起動が可能になり、関連付けられたデバイスとオブジェクトを管理できます。

始める前に

- Security Cloud Control は、Cisco Security Cloud Sign On を ID プロバイダーとして使用し、Duo を多要素認証に使用します。Cisco Security Cloud Sign On ログイン情報があり、アカウントが作成されたシスコ地域クラウドにサインインできることを確認します。
- Firewall Management Center と Cisco Security Cloud を統合するには Security Cloud Control テナントが必要です。Security Cloud Control テナントがまだない場合は、このワークフロー中にテナントをリクエストするか、作成します。詳細については、「Security Cloud Control テナントをリクエストする」を参照してください。
- Management Center のオンボーディングに使用する Security Cloud Control テナントを、Security Services Exchange（SSE）アカウントにリンクします。詳細については、「Cisco Security Cloud Control のファイアウォール を Cisco XDR テナントアカウントにリンクする」を参照してください。
- このタスクを実行するには、Firewall Management Center がバージョン 7.0.2 ～ 7.0.x、またはバージョン 7.2 以降である必要があります。

手順

ステップ 1 Firewall Management Centerで、**[統合（Integration）]** > の順に選択します。

ステップ 2 [現在のリージョン（Current Region）] ドロップダウンリストからシスコ地域クラウドを選択します。

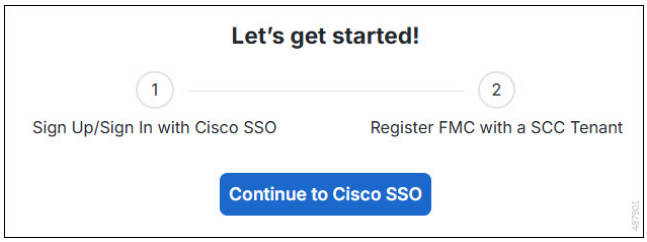
（注）
- ここで選択した地域クラウドは、Cisco Success Network および Cisco Support Diagnostics 機能にも使用されます。この設定は、シスコのセキュリティ分析とロギング（SaaS）を使用する Secure Network Analytics クラウドのクラウド地域も管理します。
- Firewall Management Center をすでにスマートライセンスに登録している場合、デフォルトで選択されるリージョンがスマートライセンスのリージョンに対応します。この場合、リージョンを変更する必要はありません。

ステップ 3 **[有効化（Enable）] Cisco Security Cloud** の順に選択します。

Security Cloud Control アカウントにログインするための別のブラウザタブが開きます。このページがポップアップブロッカーによってブロックされていないことを確認してください。

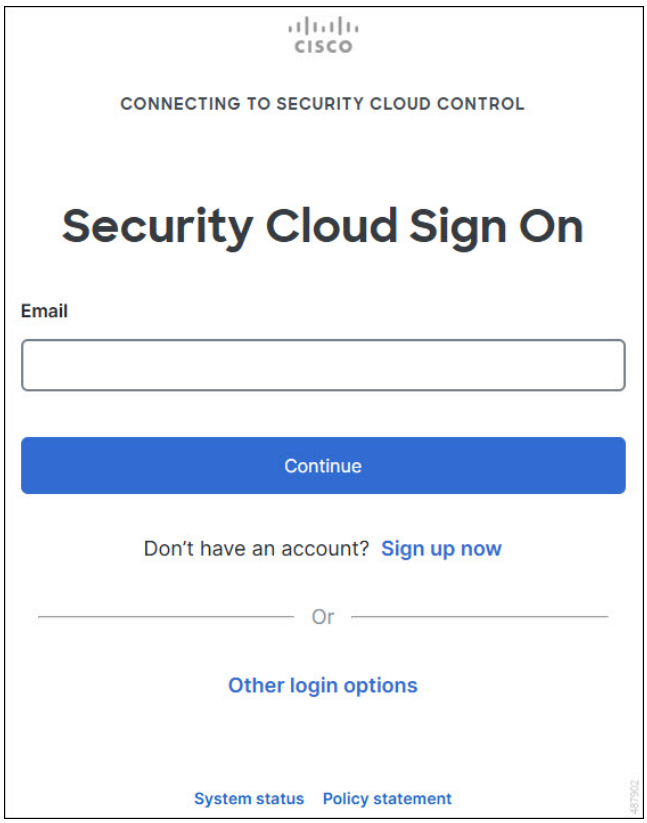
ステップ 4 [Cisco SSOに進む（Continue to Cisco SSO）] をクリックします。

図 *1 : Cisco Security Cloud* ようこそページ



ステップ 5 Security Cloud Control アカウントにログインします。

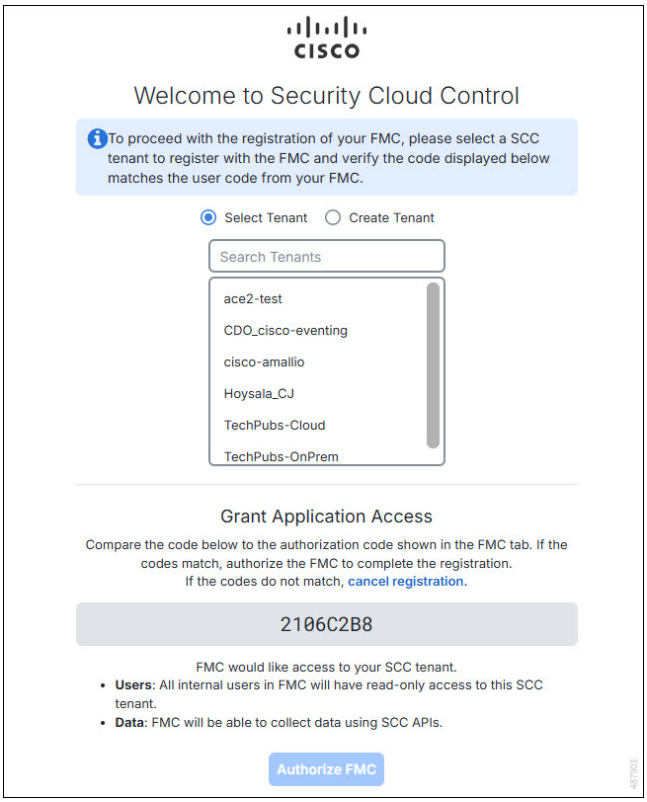
図 *2 : Security Cloud Control* サインオン



Security Cloud Control にログインするための Security Cloud Sign On アカウントがなく、アカウントを作成する場合は、[Security Cloud Sign On] ページで [今すぐ登録（Sign up now）] をクリックします。「Create a New Cisco Security Cloud Sign On Account」を参照してください。

ステップ 6 この統合に使用する Security Cloud Control テナントを選択します。Firewall Management Center と管理対象デバイスは、ここで選択した Security Cloud Control テナントにオンボーディングされます。

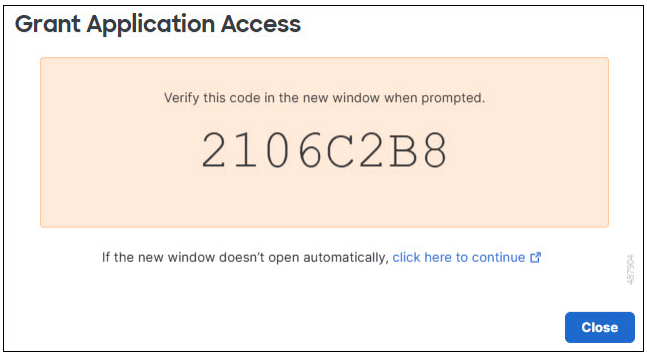
図 *3 : Security Cloud Control* テナントを選択します。



Security Cloud Control テナントがまだない場合、またはこの統合に新しいテナントを使用する場合は、新しいテナントを作成します。詳細については、「Request a Security Cloud Control Tenant」[英語] を参照してください。

ステップ 7 Security Cloud Control ログインページに表示されるコードが、Firewall Management Center で提供されるコードと一致することを確認します。

図 *4 : Firewall Management Center* の確認コード



ステップ 8 [FMCの許可（Authorize FMC）] をクリックします。

ステップ 9 Firewall Management Centerで、次のように設定します。

- [イベントの設定（Event Configuration）]：Firewall Threat Defense デバイスがイベントをクラウドに直接送信できるようにするには、この設定を有効にします。このページで設定されたイベントタイプは、適用可能で有効になっている場合、複数の統合に使用できます。詳細については、「Cisco Security Cloud にイベント送信できるようにする」を参照してください。
- [Cisco AI Assistant for Security]：Firewall Management Center に関連付けられているさまざまなタスクの支援を受けるには、Cisco AI Assistant を有効にします。詳細については、Cisco AI Assistant for Security を使用した Firewall Threat Defense デバイスの効果的な管理 （8 ページ） を参照してください。
- **[ポリシーアナライザとオプティマイザ（Policy Analyzer and Optimizer）]**：冗長ルールやシャドウルールなどの異常に対するアクセス コントロール ポリシーを評価し、検出された異常を修正するアクションを実行するには、このオプションを有効にします。詳細については、『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「ポリシーアナライザとオプティマイザを使用して異常を特定して修正する」項を参照してください。
- [Cisco Security Cloudサポート（Cisco Security Cloud Support）]：Cisco Success Network および Cisco Support Diagnostics 機能を有効にして、カスタマー サクセス イニシアチブに参加し、サポートエクスペリエンスを強化します。詳細については、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 （9 ページ）および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 （11 ページ）を参照してください。
- [Cisco XDR自動化（Cisco XDR Automation）]：この機能を有効にすると、Cisco XDR ユーザーが作成した自動ワークフローが Firewall Management Center リソースと連携できるようになります。詳細については、Cisco XDR 自動化を使用した脅威の分析と対応 を参照してください。
- **[ゼロタッチプロビジョニング（ZTP）（Zero-Touch Provisioning (ZTP)）]**：シリアル番号で Firewall Management Center にデバイスを登録する場合は、ゼロタッチプロビジョニングを有効にします。シリアル番号とアクセス コントロール ポリシーを使用して 1 つのデバイスを登録することも、シリアル番号と、事前プロビジョニングが設定されたデバイステンプレートを使用して複数のデバイスを一度に登録することもできます。詳細については、『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「シリアル番号とデバイステンプレートを使用してデバイスを追加する」項を参照してください。

ステップ 10 [保存（Save）] をクリックします。

Firewall Management Center のクラウド導入準備ステータスの表示

Cisco Security Cloud 統合を有効にすると、選択した Security Cloud Control テナントに Firewall Management Center が導入準備されます。オンボーディングタスクのステータスを表示するに

は、**Cisco Security Cloud[統合（Integration）]**ページの **クラウド導入準備ステータス** を参照してください。

次の表で、クラウド導入準備ステータスについて説明します。

表 *1*:クラウド導入準備ステータス

ステータス	説明
Online	Firewall Management Center が Security Cloud Control に導入準備されます。
オンボーディング	クラウド導入準備タスクが進行中です。これが完了するまでに最大 10 分かかる場合があります。
Security Cloud Control でのエラー	Firewall Management Center のクラウドへの導入準備中に Security Cloud Control でエラーが発生しました。 しばらくしてから Cisco Security Cloud 統合の有効化を試みてください。
使用不可（Not Available）	Firewall Management Center が Security Cloud Control から削除されたか、またはクラウド導入準備タスクがまだ始まっておらず、Security Cloud Control はまだ Firewall Management Center を検出していません。 Cisco Security Cloud を再度有効にしてみてください。
[到達不能（Unreachable）]：導入準備済みですが、現在 Management Center と通信できません	Firewall Management Center は Security Cloud Control に正常に導入準備されましたが、 Security Cloud Control は Firewall Management Centerと通信できません。 Security Cloud Control から、Firewall Management Center への再接続を試行します。詳細については、Cisco Security Cloud Control のファイアウォール を使用したオンプレミス Firewall Management Center の管理を参照してください。
ステータスの取得に失敗しました	クラウド接続エラーにより、 Firewall Management Center は Security Cloud Control からステータスを取得できませんでした。 しばらくしてから **Cisco Security Cloud[統合（Integration）]** ページを更新してステータスを確認してください。問題が解決しない場合は、 Cisco Security Cloud を再度有効にしてみてください。

（注） Cisco Security Cloud の統合を有効にした後、 Firewall Management Center を Cisco Security Cloud に登録し終えるまで最大 90 秒かかる場合があります。Cisco Security Cloud の統合を有効にした後、**[クラウドオンボーディングステータス（Cloud Onboarding Status）]** が表示されない場合は、**[Cisco Security Cloudの統合（Cisco Security Cloud Integration）]** ページを更新してください。

Cisco AI Assistant for Security を使用した Firewall Threat Defense デバイスの効果的な管理

Firewall Management Center の Cisco AI Assistant for Security は、生成型人工知能と自然言語処理テクノロジーに基づいて構築されています。これは、次の目的で使用できます。

- Firewall Management Center に関連付けられているさまざまなタスクの支援を求めます。
- 設定がベストプラクティスとセキュリティ要件に準拠していることを確認します。
- ポリシーの説明を入力し、ポリシーのコンポーネントと属性を特定します。

（注）
- AI アシスタントは、Firewall Management Center 管理者のみが使用できます。
- 現在、AI アシスタントは、Security Cloud のヨーロッパおよびアジア（APJC）地域では使用できません。ただし、将来的にはこれらの地域で使用できるようになります。最新の更新については、リリースノート を参照してください。

Cisco AI Assistant for Security を有効にする

始める前に

- Firewall Management Center の管理者権限があることを確認します。
- Firewall Management Center で Cisco Security Cloud（**[統合（Integration）]**>）が有効になっていることを確認します。

手順

ステップ 1 **[新規統合（New Integration）]**> をクリックします。

ステップ 2 **Cisco AI Assistant for Security** セクションで、[Cisco AI Assistant for Securityの有効化（Enable Cisco AI Assistant for Security）] チェックボックスをオンにします。

AI アシスタントを有効にすると、Firewall Management Center メニューバーに AI アシスタント（）が表示されます。

Cisco AI Assistant for Security を使用したサポートの要請

始める前に

- Firewall Management Center の管理者権限があることを確認します。
- Firewall Management Center で Cisco AI Assistant for Security（**[統合（Integration）]**>>**[Cisco AI Assistant for Security の有効化（Enable Cisco AI Assistant for Security）]**）が有効になっていることを確認します。

手順

ステップ 1 Firewall Management Center メニューバーで、**[Cisco AI Assistant for Security]**（[）をクリックします。

AI アシスタントを初めて開くと、カルーセルウィンドウが表示されます。

ステップ 2 （1 回限りのアクティビティ）カルーセルウィンドウでコンテンツを確認し、[AIアシスタントの起動（Launch AI Assistant）] をクリックします。

ステップ 3 AI アシスタントウィンドウで、利用可能な提案のいずれかを選択するか、テキストフィールドに独自の質問を入力し、[メッセージの送信（Send Message）]（）をクリックします。

詳細については、AI Assistant ユーザーガイドを参照してください。

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

Cisco Success Network は、Firewall Management Center を有効にして Cisco Cloud とのセキュアな接続を確立するクラウドサービスで、使用情報と統計情報がストリーミングされます。このテ

レメトリをストリーミングすることによって、次の理由で、Firewall Threat Defense デバイスから対象のデータを選択して構造化形式でリモートの管理ステーションに送信するメカニズムが提供されます。

- ネットワーク内の製品の有効性を向上させるために、使用可能でありながら未使用の機能について通知します。
- 製品に利用可能な、追加のテクニカルサポートサービスとモニタリングについて通知します。
- シスコ製品の改善に役立ちます。

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 Secure Firewall Management Center デバイスによって収集される Cisco Success Network テレメトリデータ [英語] を参照してください。

（注）
- Cisco Success Network は評価モードではサポートされていません。
- Cisco Success Networkはデフォルトで有効になっています。
- Firewall Management Center が有効な Smart Software Manager オンプレミス（旧称：Smart Software Satellite Server）構成または特定のライセンス予約を使用する場合は、Cisco Success Network はサポートされません。

始める前に

Cisco Security Cloud統合を有効にするか、Firewall Management Center をスマートライセンスに登録して、このタスクを実行します。

手順

ステップ 1 **[統合（Integration）]** > **[Cisco Security Cloud]** の順に選択します。

ステップ 2 **[Cisco Security Cloudサポート（Cisco Security Cloud Support）]**で、**[Cisco Success Networkを有効にする（Enable Cisco Success Network）]** チェックボックスをオンにして、このサービスを有効にします。

（注）
続行する前に、[Cisco Success Networkを有効化（Enable Cisco Success Network）] チェックボックスの横にある情報を読んでください。

ステップ 3 [保存（Save）] をクリックします。

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

Cisco Support Diagnostics は、Firewall Management Center と管理対象デバイスを有効にして、Cisco Cloud とのセキュアな接続を確立し、デバイスの正常性に関する情報をクラウドに送信するクラウドベースの TAC サポートサービスです。この機能は、デフォルトでイネーブルにされています。

Cisco Support Diagnostics は、Cisco TAC が TAC ケースの解決中にデバイスから重要なデータを安全に収集できるようにすることで、トラブルシューティングの際によりよいユーザーエクスペリエンスを提供します。さらに、シスコは自動問題検出システムによって定期的にヘルスデータを収集および処理し、問題がある場合はユーザーに通知します。TAC ケース解決時のデータ収集サービスはサポート契約を持つすべてのユーザーが利用できますが、通知サービスは、特定のサービス契約を持つユーザーのみが使用できます。

Cisco Support Diagnostics を使用すると、Firewall Threat Defense デバイスと Firewall Management Center の両方で Cisco Cloud とのセキュアな接続が確立されて維持されます。Firewall Management Center は、収集したデータを **[Cisco Security Cloud統合（Cisco Security Cloud Integration）]** ページで選択された地域クラウドに送信します。

管理者が Firewall Management Center から収集されたデータのサンプルファイルを表示するには、「特定のシステム機能に関するトラブルシューティング ファイルの生成」に従います。

始める前に

Cisco Security Cloud統合を有効にするか、Firewall Management Center をスマートライセンスに登録して、このタスクを実行します。

手順

ステップ 1 **[統合（Integration）]** > **[Cisco Security Cloud]** を選択します。

ステップ 2 **[Cisco Security Cloudサポート（Cisco Security Cloud Support）]**で、**[Cisco サポート診断を有効にする（Enable Cisco Support Diagnostics）]** チェックボックスをオンにして、このサービスを有効にします。

（注）
続行する前に、[Cisco Support Diagnosticsを有効化（Enable Cisco Support Diagnostics）] チェックボックスの横にある情報を読んでください。

ステップ 3 [保存（Save）] をクリックします。

システム構成の要件と前提条件

モデルのサポート

Management Center

サポートされるドメイン

Global

ユーザの役割

管理者

Secure Firewall Management Center システム設定の管理

システム コンフィギュレーションは、Firewall Management Center の基本設定を識別します。

手順

ステップ 1 [システム（System）]（⚙）>**[構成（Configuration）]**を選択します。

ステップ 2 ナビゲーションウィンドウを使用して、変更する設定を選択します。

アクセス リスト

IP アドレスとポートによって FMC へのアクセスを制限できます。デフォルトでは、任意の IP アドレスに対して以下のポートが有効化されています。

- 443（HTTPS）：Web インターフェイス アクセスに使用されます。
- 22（SSH）：CLI アクセスに使用されます。

さらに、ポート 161 で SNMP 情報をポーリングするためのアクセスも追加できます。SNMP はデフォルトで無効になっているため、SNMP アクセスルールを追加する前に、まず SNMP を有効にする必要があります。詳細については、SNMP ポーリングの設定 （82 ページ）を参照してください。

注意 デフォルトでは、アクセスは制限されていません。よりセキュアな環境で運用するために、特定の IP アドレスに対するアクセスを追加してから、デフォルトの **any** オプションを削除することを検討してください。

アクセス リストの設定

このアクセス リストは、外部データベース アクセスを制御しません。データベースへの外部アクセスの有効化 （36 ページ）を参照してください。

注意 Firewall Management Center への接続に現在使用されている IP アドレスへのアクセスを削除して、「`IP=any port=443`」のエントリが存在しない場合、保存した時点でアクセスは失われます。

始める前に

デフォルトでは、アクセスリストには HTTPS と SSH のルールが含まれています。SNMP ルールをアクセスリストに追加するには、まず SNMP を有効にする必要があります。詳細については、「SNMP ポーリングの設定 （82 ページ）」を参照してください。

手順

ステップ 1 [システム（System）]（⚙）>**[構成（Configuration）]** を選択します。

ステップ 2 （オプション）SNMP ルールをアクセスリストに追加する場合は、[SNMP] をクリックして SNMP を設定します。デフォルトでは、SNMP は無効になっています。SNMP ポーリングの設定 （82 ページ） を参照してください。

ステップ 3 [アクセス リスト（Access List）] をクリックします。

ステップ 4 1 つ以上の IP アドレスへのアクセスを追加するには、[ルールの追加（Add Rules）] をクリックします。

ステップ 5 [IP アドレス（IP Address）] フィールドに、IP アドレスまたはアドレスの範囲を入力するか、`any` を入力します。

ステップ 6 [SSH]、[HTTPS]、[SNMP]、またはこれらのオプションの組み合わせを選択して、これらの IP アドレスで有効にするポートを指定します。

ステップ 7 [追加（Add）] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

関連トピック

Firepower システムの IP アドレス表記法

アクセス コントロールの設定

[システム（System）]（⚙）>**[設定（Configuration）]**>**[アクセスコントロールの設定（Access Control Preferences）]** でアクセス制御の設定を指定します。

ルール変更に関するコメントの要求

ユーザーが保存時にコメントすることを許可（または要求）することで、アクセス制御ルールの変更を追跡できます。これにより、展開内の重要なポリシーが変更された理由をすばやく評価できます。デフォルトでは、この機能はディセーブルになっています。

オブジェクトの最適化

ルールポリシーをファイアウォールデバイスに展開すると、関連付けられたネットワーク オブジェクト グループをデバイス上に作成するときに、ルールで使用するネットワーク/ホストポリシーオブジェクトを評価して最適化するようにFirewall Management Centerを設定できます。最適化によって、隣接するネットワークがマージされ、冗長なネットワーク エントリが削除されます。これにより、実行時のアクセスリストデータ構造と設定のサイズが縮小されます。メモリ制約のある一部のファイアウォールデバイスでは、これによるメリットがあります。

たとえば、次のエントリを含みアクセスルール内で使用されるネットワーク/ホストオブジェクトについて考えてみます。

```
192.168.1.0/24
192.168.1.23
10.1.1.0
10.1.1.1
10.1.1.2/31
```

最適化が有効になっている場合、ポリシーを展開すると、結果のオブジェクトグループ設定が生成されます。

```
object-group network test
description (Optimized by management center)
network-object 10.1.1.0 255.255.255.252
network-object 192.168.1.0 255.255.255.0
```

最適化が無効になっている場合、グループ設定は次のようになります。

```
object-group network test
network-object 192.168.1.0 255.255.255.0
network-object 192.168.1.23 255.255.255.255
network-object 10.1.1.0 255.255.255.255
network-object 10.1.1.1 255.255.255.255
network-object 10.1.1.2 255.255.255.254
```

この最適化によってネットワーク/ホストオブジェクトの定義が変更されることも、新しいネットワーク/ホスト ポリシー オブジェクトが作成されることもありません。ネットワーク オブジェクト グループに別のネットワーク、ホストオブジェクト、またはオブジェクトグループが含まれている場合、オブジェクトは結合されません。代わりに、各ネットワーク オブジェクト グループが個別に最適化されます。また、展開中の最適化プロセスの一環として、ネットワーク オブジェクト グループのインライン値のみが変更されます。

重要 最適化は、Firewall Management Center で機能が有効になった後の「最初の展開時」に「管理対象デバイス」で行われます。ルールの数が多い場合、システムがポリシーを評価してオブジェクトの最適化を実行するのに数分から1時間かかることがあります。この間、デバイスのCPU使用率も高くなることがあります。機能が無効になった後の最初の展開でも同様のことが発生します。この機能が有効または無効になった後は、メンテナンス時間帯やトラフィックの少ない時間帯など、影響が最小限になる時間に展開することを強く推奨します。

この機能は、デフォルトで有効になっています。無効にすることもできますが、有効のままにしておくことをお勧めします。

監査ログ

Firewall Management Center は、ユーザーのアクティビティを読み取り専用監査ログに記録します。監査ログのデータは、いくつかの方法で確認できます。

- Web インターフェイスを使用します： 監査と Syslog。

  監査ログは標準イベントビューに表示され、監査ビュー内の任意の項目に基づいて監査ログメッセージを表示、ソート、およびフィルタリングできます。監査情報を簡単に削除したり、それに関するレポートを作成したりすることができ、ユーザーが行った変更に関する詳細なレポートを表示することもできます。

- syslog への監査ログ メッセージのストリーミング：syslog への監査ログのストリーミング（16 ページ）。

- HTTP サーバーへの監査ログ メッセージのストリーミング：HTTP サーバーへの監査ログのストリーミング （18 ページ）。

監査ログデータを外部サーバーにストリーミングすると、Firewall Management Center の容量を節約できます。 外部 URL に監査情報を送信すると、システム パフォーマンスに影響を与える場合があるので注意してください。

オプションで監査ログストリーミングのチャネルを保護するには、TLS証明書を使用してTLSおよび相互認証を有効にします。監査ログ証明書 （19 ページ）を参照してください。

複数の syslog サーバーへのストリーミング

監査ログデータは、最大 5 つの syslog サーバーにストリーミングできます。ただし、保護された監査ログストリーミングに対して TLS を有効にしている場合は、1 つの syslog サーバーにのみストリーミングできます。

設定変更の syslog へのストリーミング

構成データの形式とホストを指定することにより、構成変更を監査ログデータの一部として syslog にストリーミングできます。Firewall Management Center は、監査構成ログのバックアップと復元をサポートしています。高可用性の場合、アクティブなFirewall Management Centerのみが設定変更 syslog を外部 syslog サーバーに送信します。ログファイルは HA ペア間で同期さ

れるため、フェールオーバーまたはスイッチオーバー時には新しいアクティブ Firewall Management Center が変更ログの送信を再開します。HA ペアがスプリットブレインモードで動作している場合は、ペアの両方の Firewall Management Center が設定変更 syslog を外部サーバーに送信します。

syslog への監査ログのストリーミング

この機能を有効にすると、監査ログレコードは、syslog に次の形式で表示されます。

```
Date Time Host: [Tag] Sender: User_Name@User_IP, Subsystem, Action
```

現地の日付、時刻、および発信元ホスト名の後に、角括弧で囲まれたオプション タグが続き、送信側デバイス名の後に監査ログ メッセージが続きます。

たとえば、Management Center からの監査ログメッセージに `FMC-AUDIT-LOG` のタグを指定すると、Firewall Management Center からのサンプル監査ログメッセージは次のように表示されます。

```
Mar 01 14:45:24 localhost: [FMC-AUDIT-LOG] Dev-MC7000: admin@10.1.1.2, Operations >
Monitoring, Page View
```

重大度とファシリティを指定する場合、これらの値は syslog メッセージに表示されません。代わりに、これらの値は、syslog メッセージを受信するシステムにメッセージの分類方法を示します。

始める前に

Firewall Management Center が syslog サーバーと通信できることを確認します。設定を保存すると、システムは ICMP/ARP パケットと TCP SYN パケットを使用して syslog サーバーが到達可能であることを確認します。次に、システムのデフォルトでは、ポート 514/UDP を使用して監査ログがストリーミングされます。チャネルを保護する場合（任意、監査ログ証明書 （19 ページ）を参照）、TCP 用にポート 1470 を手動で設定する必要があります。

手順

ステップ 1 [システム（System）]（⚙）> **[構成（Configuration）]** を選択します。

ステップ 2 [監査ログ（Audit Log）] をクリックします。

ステップ 3 [監査ログを Syslog に送信（Send Audit Log to Syslog）] ドロップダウン メニューから、[有効化（Enabled）] を選択します。

ステップ 4 次のフィールドは、syslog に送信される監査ログにのみ適用されます。

オプション	説明
設定変更の送信	設定変更の syslog を監査ログストリーミングに含めるには、ドロップダウンから関連するオプションを選択します。 • JSON：syslog には設定変更の詳しい相違点が含まれます。 • API：syslog には、設定変更の詳しい相違点を取得するための API が含まれます。 • なし：設定変更の詳細情報を除く、他のすべての監査ログを保持します。
ホスト（Host）	監査ログの送信先となる syslog サーバーの IP アドレスまたは完全修飾名。最大 5 つの syslog ホストをカンマで区切って追加できます。 （注） 監査サーバー証明書で TLS が無効になっている場合にのみ、複数の syslog ホストを指定できます。
ファシリティ	メッセージを作成するサブシステム。 Syslog アラート ファシリティ で説明されているファシリティを選択します。たとえば、AUDIT を選択します。
Severity	メッセージの重大度。 syslog 重大度レベル で説明されている重大度を選択します。
タグ	監査ログ syslog メッセージに含めるオプションのタグ。 ベストプラクティス：このフィールドに値を入力すると、監査ログメッセージと他の類似した syslog メッセージ（ヘルスアラートなど）を簡単に区別できます。 たとえば、syslog に送信されるすべての監査ログレコードに `FMC-AUDIT-LOG` でラベル付けする場合は、このフィールドに `FMC-AUDIT-LOG` と入力します。

ステップ 5 （任意）syslog サーバーの IP アドレスが有効であるかどうかをテストするには、[syslogサーバーのテスト（Test Syslog Server）] をクリックします。

システムは、syslog サーバーが到達可能かどうかを確認するために次のパケットを送信します。

1. ICMP エコー要求
2. 443 ポートと 80 ポートで TCP SYN
3. ICMP タイムスタンプクエリ
4. ランダムポートで TCP SYN

（注）
Firewall Management Center と syslog サーバーが同じサブネットにある場合は、ICMP の代わりに ARP が使用されます。

システムに、各サーバーの結果が表示されます。

ステップ 6 [保存（Save）] をクリックします。

HTTP サーバーへの監査ログのストリーミング

この機能を有効にすると、アプライアンスは、HTTP サーバーに次の形式で監査ログ レコードを送信します。

```
Date Time Host: [Tag] Sender: User_Name@User_IP, Subsystem, Action
```

ローカルの日付、時刻、および発信元ホスト名の後に、角括弧で囲まれたオプション タグが続き、送信側アプライアンス名の後に監査ログ メッセージが続きます。

たとえば、FROMMC のタグを指定した場合は、監査ログメッセージ例は次のように表示されます。

```
Mar 01 14:45:24 localhost: [FROMMC] Dev-MC7000: admin@10.1.1.2, Operations > Monitoring, Page View
```

始める前に

デバイスが HTTP サーバーと通信できることを確認します。オプションで、チャネルを保護します。監査ログ証明書 （19 ページ）を参照してください。

手順

ステップ 1 [システム（System）]（⚙）>**[構成（Configuration）]** を選択します。

ステップ 2 [監査ログ（Audit Log）] をクリックします。

ステップ 3 必要に応じて、[タグ（Tag）] フィールドに、メッセージとともに表示するタグ名を入力します。たとえば、すべての監査ログ レコードの前に FROMMC を付けるには、このフィールドに FROMMC を入力します。

ステップ 4 [HTTP サーバーへの監査ログの送信（Send Audit Log to HTTP Server）] ドロップダウン リストから、[有効（Enabled）] を選択します。

ステップ 5 [監査情報を送信する URL（URL to Post Audit）] フィールドに、監査情報の送信先 URL を指定します。次にリストした HTTP POST 変数を要求するリスナー プログラムに対応する URL を入力します。

- subsystem
- actor
- event_type

- `message`
- `action_source_ip`
- `action_destination_ip`
- 結果
- `time`
- `tag`（定義されている場合。手順 3 を参照）

注意
暗号化されたポストを許可するには、HTTPS URL を使用します。外部 URL に監査情報を送信すると、システム パフォーマンスに影響を与える場合があります。

ステップ 6 [保存（Save）] をクリックします。

監査ログ証明書

Transport Layer Security（TLS）証明書を使用して、Firewall Management Center と信頼できる監査ログサーバー間の通信を保護することができます。

クライアント証明書（必須）

証明書署名要求（CSR）を生成して、署名のために認証局（CA）に送信してから、署名付き証明書を Firewall Management Center にインポートする必要があります。ローカルシステム設定を使用します。Firewall Management Center の署名付き監査ログ クライアント証明書の取得（21 ページ） および Firewall Management Center への監査ログ クライアント証明書のインポート（22 ページ）。

サーバー証明書（オプション）

セキュリティを強化するために、Firewall Management Center と監査ログサーバー間の相互認証を要求することを推奨します。相互認証を実現するには、1 つ以上の証明書失効リスト（CRL）をロードします。これらの CRL にリストされている失効した証明書を使用して、サーバーに監査ログをストリーミングすることはできません。

Cisco Secure Firewall は、識別符号化規則（DER）形式でエンコードされた CRL をサポートしています。これらの CRL は、システムが Firewall Management Center Web インターフェイスの HTTPS クライアント証明書を検証するために使用する CRL と同じであることに注意してください。

ローカルシステム設定を使用します。有効な監査ログ サーバー証明書の要求（23 ページ）。

監査ログのセキュアなストリーミング

信頼できる HTTP サーバーまたは syslog サーバーに監査ログをストリーミングする場合、Transport Layer Security（TLS）証明書を使用して Firewall Management Center とサーバー間のチャネルを保護できます。監査するアプライアンスごとに一意のクライアント証明書を生成する必要があります。

始める前に

クライアントおよびサーバー証明書を必須とする場合の影響については、監査ログ証明書 （19 ページ）を参照してください。

手順

ステップ 1 署名付きクライアント証明書を入手し、Firewall Management Center にインストールします。

a) Firewall Management Center の署名付き監査ログ クライアント証明書の取得 （21 ページ）：

システム情報と指定した ID 情報に基づいて、Firewall Management Center デバイスで証明書署名要求（CSR）を生成します。

CSR を認識済みの信頼できる認証局（CA）に送信して、署名付きクライアント証明書を要求します。

Firewall Management Center と監査ログサーバー間の相互認証が必要な場合、接続に使用するサーバー証明書に署名したのと同じ CA がクライアント証明書に署名する必要があります。

b) 認証局から署名付き証明書を受信した後は、その証明書を Firewall Management Center にインポートします。Firewall Management Center への監査ログ クライアント証明書のインポート （22 ページ）を参照してください。

ステップ 2 Transport Layer Security（TLS）を使用するサーバとの通信チャネルを設定し、相互認証を有効にします。

有効な監査ログ サーバー証明書の要求 （23 ページ）を参照してください。

ステップ 3 まだ行っていない場合は、監査ログ ストリーミングを設定します。

syslog への監査ログのストリーミング （16 ページ）またはHTTP サーバーへの監査ログのストリーミング （18 ページ）を参照してください。

Firewall Management Center の署名付き監査ログ クライアント証明書の取得

重要 ハイ アベイラビリティ設定のスタンバイ Firewall Management Center では [監査ログ証明書（Audit Log Certificate）] ページを使用できません。スタンバイ Firewall Management Center からこのタスクを実行することはできません。

システムは、ベース 64 エンコードの PEM 形式で証明書要求のキーを生成します。

始める前に

次の点を考慮してください。

- セキュリティを確保するには、グローバルに認識された信頼できる認証局（CA）を使用して、証明書に署名します。
- アプライアンスと監査ログ サーバー間で相互認証が必要な場合は、同じ認証局によってクライアント証明書とサーバー証明書の両方が署名される必要があります。

手順

ステップ 1 [システム（System）]（⚙）>**[構成（Configuration）]**を選択します。

ステップ 2 [監査ログ証明書（Audit Log Certificate）] をクリックします。

ステップ 3 [新規 CSR の生成（Generate New CSR）] をクリックします。

ステップ 4 [国名（2 文字のコード）（Country Name (two-letter code)）] フィールドに国番号を入力します。

ステップ 5 [都道府県（State or Province）] フィールドに、都道府県名を入力します。

ステップ 6 [市区町村（Locality or City）] を入力します。

ステップ 7 [組織（Organization）] の名前を入力します。

ステップ 8 [組織単位（部署名）（Organizational Unit (Department)）] の名前を入力します。

ステップ 9 [共通名（Common Name）] フィールドに、証明書を要求するサーバーの完全修飾ドメイン名を入力します。

（注）
共通名と DNS ホスト名が一致しないと、監査ログのストリーミングは失敗します。

ステップ 10 [生成（Generate）] をクリックします。

ステップ 11 テキスト エディタで、新しい空のファイルを開きます。

ステップ 12 証明書要求のテキスト ブロック全体（`BEGIN CERTIFICATE REQUEST` 行と `END CERTIFICATE REQUEST` 行を含む）をコピーして、空のテキスト ファイルに貼り付けます。

ステップ 13 このファイルを *clientname*.csr として保存します。*clientname* は、証明書を使用する予定のアプライアンスの名前にします。

ステップ 14 [閉じる（Close）] をクリックします。

次のタスク

- この手順の「はじめる前に」セクションのガイドラインを使用して選択した認証局に、証明書署名要求を送信します。
- 署名された証明書を受け取ったら、アプライアンスにインポートします。Firewall Management Center への監査ログ クライアント証明書のインポート （22 ページ）を参照してください。

Firewall Management Center への監査ログ クライアント証明書のインポート

Firewall Management Center ハイアベイラビリティ設定では、アクティブピアを使用する必要があります。

始める前に

- Firewall Management Center の署名付き監査ログ クライアント証明書の取得 （21 ページ）。
- 正しい Firewall Management Center の署名付き証明書をインポートしていることを確認します。
- 証明書を生成した署名認証局から中間 CA を信頼するように要求された場合は、必要な証明書チェーン（証明書パスとも呼ばれる）を提供します。クライアント証明書に署名した CA は、証明書チェーンのいずれの中間証明書に署名した CA と同じである必要があります。

手順

ステップ 1 Firewall Management Center で、[システム（System）]（⚙）>**[構成（Configuration）]** を選択します。

ステップ 2 [監査ログ証明書（Audit Log Certificate）] をクリックします。

ステップ 3 [監査クライアント証明書のインポート（Import Audit Client Certificate）] をクリックします。

ステップ 4 テキストエディタでクライアント証明書を開いて、`BEGIN CERTIFICATE` の行と `END CERTIFICATE` の行を含むテキストのブロック全体をコピーします。このテキストを [クライアント証明書（Client Certificate）] フィールドに貼り付けます。

ステップ 5 秘密キーをアップロードするには、秘密キー ファイルを開いて、`BEGIN RSA PRIVATE KEY` の行と `END RSA PRIVATE KEY` の行を含むテキストのブロック全体をコピーします。このテキストを [秘密キー（Private Key）] フィールドに貼り付けます。

ステップ 6 必要な中間証明書をすべて開いて、それぞれのテキストのブロック全体をコピーして、[証明書チェーン（Certificate Chain）] フィールドに貼り付けます。

ステップ 7 [保存（Save）] をクリックします。

有効な監査ログ サーバー証明書の要求

システムは、識別符号化規則（DER）形式でインポートされている CRL を使用した、監査ログ サーバー証明書の検証をサポートしています。

（注） CRL を使用して証明書を確認する場合、システムは、監査ログ サーバー証明書の検証と、アプライアンスと Web ブラウザの間の HTTP 接続を保護する証明書の検証の両方に、同じ CRL を使用します。

重要 高可用性ペアのスタンバイ Firewall Management Center でこの手順を実行することはできません。

始める前に

- 相互認証を必須とし、証明書失効リスト（CRL）を使用して証明書の有効性を保持する場合の影響について説明します。監査ログ証明書 （19 ページ）を参照してください。
- 監査ログのセキュアなストリーミング （20 ページ）に記載されている手順およびその手順で参照されているトピックに従って、クライアント証明書を取得してインポートします。

手順

ステップ 1 Firewall Management Center で、[システム（System）]（⚙） > **[構成（Configuration）]** を選択します。

ステップ 2 [監査ログ証明書（Audit Log Certificate）] をクリックします。

ステップ 3 Transport Layer Security を使用して監査ログを安全に外部サーバへストリーミングするには、[TLS の有効化（Enable TLS）] 選択します。

TLS が有効になっている場合、syslog クライアント（Firewall Management Center）は、サーバーから受信した証明書を検証します。クライアントとサーバーの間の接続は、サーバー証明書の

検証が成功した場合にのみ成功します。この検証プロセスでは、次の条件を満たす必要があります。

- 証明書をクライアントに送信するように syslog サーバーを設定します。
- サーバー証明書を検証するために、CA 証明書をクライアントに追加（インポート）します。
  - クライアント証明書のインポート中に CA 証明書をインポートする必要があります。
  - 発行 CA が下位 CA の場合は、下位 CA（ルート CA）から署名 CA を追加する前に発行 CA を追加するといったことが必要になります。

ステップ 4 クライアントがサーバーに対して自分自身を認証することを望まないが、証明書が同じ CA によって発行されている場合にサーバー証明書を受け入れる場合は、次の手順を実行します（非推奨）。

a) [相互認証の有効化（Enable Mutual Authentication）] をオフにします。

重要
サーバーがクライアント証明書を検証せずにクライアントを信頼するように設定されていることを確認してください。

b) [保存（Save）] をクリックして、残りの手順をスキップします。

ステップ 5 （任意）監査ログサーバーによるクライアント証明書の検証を有効にするには、[相互認証の有効化（Enable Mutual Authentication）] をオンにします。

重要
[相互認証の有効化（Enable Mutual Authentication）] オプションは、TLS が有効になっている場合にのみ適用されます。

相互認証が有効になっている場合、syslog クライアント（Firewall Management Center）は、検証のためにクライアント証明書を syslog サーバーに送信します。クライアントは、syslog サーバーのサーバー証明書に署名した CA の同じ CA 証明書を使用します。接続は、クライアント証明書の検証が成功した場合にのみ成功します。この検証プロセスでは、次の条件を満たす必要があります。

- クライアントから受信した証明書を検証するように syslog サーバーを設定します。
- syslog サーバーに送信するクライアント証明書を追加します。この証明書は、syslog サーバーのサーバー証明書に署名した CA によって署名されている必要があります。

（注）
syslog サーバーへの監査ログのストリーミングに相互認証を使用する場合は、秘密キーに PKCS#1 形式ではなく PKCS#8 形式を使用します。PKCS#1 キーを PKCS#8 形式に変換するには、次のコマンドラインを使用してください。

```
openssl pkcs8 -topk8 -inform PEM -outform PEM
-nocrypt -in PKCS1 key file name -out PKCS8 key filename
```

ステップ 6 （任意）無効になっているサーバー証明書を自動的に認識するには、次の手順を実行します。

a) [CRLの取得の有効化（Enable Fetching of CRL）] をオンにします。

重要
このオプションは、[相互認証の有効化（Enable Mutual Authentication）] チェックボックスがオンになっている場合にのみ表示されます。ただし、[CRLの取得の有効化（Enable Fetching of CRL）] オプションは、TLS オプションが有効になっている場合にのみ適用されます。CRL の使用目的はサーバー証明書の検証であり、クライアント証明書の検証を可能にするための相互認証の使用には依存しません。

CRL の取得を有効にすると、定期的に CRL を更新（ダウンロード）するクライアントのスケジュールタスクが作成されます。CRL はサーバー証明書の検証に使用され、検証対象のサーバー証明書が CA によって取り消されたことを示す CA からの CRL がある場合、検証は失敗します。

b) 既存の CRL ファイルへの有効な URL を入力して、[CRL の追加（Add CRL）] をクリックします。

最大 25 個まで CRL の追加を繰り返します。

c) [CRL の更新（Refresh CRL）] をクリックして現在の CRL をロードするか、指定した URL から CRL をロードします。

ステップ 7 クライアント証明書を作成したものと同じ認証局によって生成された有効なクライアント証明書があることを確認します。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

（オプション）CRL 更新の頻度を設定します。 証明書失効リストのダウンロードの設定を参照してください。

Firewall Management Center での監査ログ クライアント証明書の表示

ログインしているアプライアンスの監査ログ クライアント証明書のみ表示できます。Firewall Management Center高可用性ペアでは、アクティブ ピアでのみ証明書を表示できます。

手順

ステップ 1 [システム（System）]（⚙）>**[構成（Configuration）]**を選択します。

ステップ 2 [監査ログ証明書（Audit Log Certificate）] をクリックします。

変更調整

ユーザが行う変更をモニタし、変更が部門の推奨する標準に従っていることを確認するため、過去 24 時間に行われたシステム変更の詳細なレポートを電子メールで送信するようにシステムを構成できます。ユーザが変更をシステム構成に保存するたびに、変更のスナップショットが取得されます。変更調整レポートは、これらのスナップショットによる情報を組み合わせて、最近のシステム変更の概要を提供します。

次の図は、変更調整レポートの [ユーザー（User）] セクションの例を示しています。ここには、各構成の変更前の値と変更後の値の両方が一覧表示されています。ユーザが同じ構成に対して複数の変更を行った場合は、個々の変更の概要が最新のものから順に時系列でレポートに一覧表示されます。

過去 24 時間に行われた変更を参照できます。

変更調整の設定

始める前に

- 24 時間にシステムに行われた変更のメール送信されるレポートを受信する電子メールサーバーを設定します。詳細については、メール リレー ホストおよび通知アドレスの設定（34 ページ）を参照してください。

手順

ステップ 1 [システム（System）]（⚙）>**[構成（Configuration）]**を選択します。

ステップ 2 [変更調整（Change Reconciliation）] をクリックします。

ステップ 3 **[有効（Enable）]** チェックボックスをオンにします。

ステップ 4 [実行する時間（Time to Run）] ドロップダウン リストから、システムが変更調整レポートを送信する時刻を選択します。

ステップ 5 [メール宛先（Email to）] フィールドにメール アドレスを入力します。

ヒント
電子メール アドレスを追加したら、いつでも [最新のレポートの再送信（Resend Last Report）] をクリックして、最新の変更調整レポートのコピーを受信者に再送信できます。

ステップ 6 ポリシーの変更を追加する場合は、[ポリシー設定を含める（Include Policy Configuration）] チェックボックスをオンにします。

ステップ 7 過去 24 時間のすべての変更を含める場合は、[全変更履歴を表示（Show Full Change History）] チェックボックスをオンにします。

ステップ 8 [保存（Save）] をクリックします。

関連トピック

監査ログを使って変更を調査する

変更調整オプション

[ポリシー設定を含める（Include Policy Configuration）] オプションは、ポリシーの変更のレコードを変更調整レポートに含めるかどうかを制御します。これには、アクセス制御、侵入、システム、ヘルス、およびネットワーク検出の各ポリシーの変更が含まれます。このオプションを選択しなかった場合は、ポリシーの変更はどれもレポートに表示されません。このオプションは Firewall Management Center のみで使用できます。

[すべての変更履歴を表示する（Show Full Change History）] オプションは、過去 24 時間のすべての変更のレコードを変更調整レポートに含めるかどうかを制御します。このオプションを選択しなかった場合は、変更がカテゴリごとに統合された形でレポートに表示されます。

（注） 変更調整レポートには、Firewall Threat Defense インターフェイスおよびルーティング設定への変更は含まれません。

変更管理

変更を展開する前の監査追跡や正式な承認など、設定変更に関してより正式なプロセスを実装する必要がある組織の場合は、変更管理を有効にできます。

変更管理を有効にすると、[チケット（Ticket）]（） のショートカットがメニューバーに追加され、[変更管理ワークフロー（Change Management Workflow）] が [システム（System）]（） メニューに追加されます。ユーザーは、これらの方法を使用してチケットを管理できます。

詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドの「Change Management」の章を参照してください。

[システム（System）]（） > **[構成（Configuration）]** ページでは、次の設定を指定することができます。[保存（Save）] をクリックして変更を保存します。

- [変更管理の有効化（Enable Change Management）]：チケットと変更管理ワークフローを有効にします。有効にした場合、変更管理を無効にするには、すべてのチケットを承認または破棄する必要があります。

  この機能を無効にするには、オプションをオフにします。変更管理を無効にするには、すべてのチケットを承認または破棄する必要があります。いずれかのチケットが [処理中（In Progress）]、[保留中（On Hold）]、[拒否（Rejected）]、または [承認保留中（Pending Approval）] 状態になっている場合は、変更管理を無効にできません。

- [必要な承認の数（Number of approvals required）]：チケットを承認して展開可能にするために、変更を承認する必要がある管理者の人数。デフォルトは1人ですが、チケットごとに最大5人の承認者を要求できます。ユーザーは、チケットの作成時にこの数を上書きできます。

（注） 変更管理が有効になっており、使用中の場合、少なくとも 1 つのチケットが [処理中（In Progress）]、[保留中（On Hold）]、[拒否（Rejected）]、または [承認保留中（Pending Approval）] 状態になっていると、承認者の人数を変更できません。必要な承認者数を変更するには、すべてのチケットを承認または破棄する必要があります。

- [チケットの消去期間（Ticket Purge Duration）]：承認されたチケットを保持する日数（1 ～ 100 日）。デフォルトは 5 日間です。
- [電子メール通知（Email Notification）]（任意）：[返信先アドレス（Reply to Address）] と、[承認者アドレスのリスト（List of Approver Addresses）] の電子メールアドレスを入力します。電子メールを機能させるには、電子メール通知のシステム設定も指定する必要があります。

  クラウド提供型 Firewall Management Center の場合、返信先アドレスは表示されません。代わりに、電子メール通知のシステム設定でこのアドレスを指定してください。

注記

変更管理の有効化/無効化を妨げるシステムプロセスがいくつかあります。次のいずれかが処理中の場合は、これらの設定を変更する前に、それらが完了するまで待つ必要があります：バックアップ/復元、インポート/エクスポート、ドメインの移動、アップグレード、Flexconfig の移行、デバイスの登録、高可用性の登録/作成/解除/切り替え、クラスタノードの作成/登録/解除/編集/追加/削除、EPM のブレークアウト/参加。

これらの設定を変更した場合、アクセス コントロール ポリシーをロックすることはできません。ポリシーがロックされている場合は、この機能を有効または無効にする前に、ロックが解除されるまで待つ必要があります。

DNS キャッシュ

イベント表示ページで、IP アドレスを自動的に解決するようにシステムを設定できます。また、アプライアンスによって実行される DNS キャッシュの基本的なプロパティを設定できます。DNS キャッシングを設定すると、追加のルックアップを実行せずに、以前に解決した IP アドレスを識別できます。これにより、IPアドレスの解決が有効になっている場合に、ネットワーク上のトラフィックの量を減らし、イベントページの表示速度を速めることができます。

DNS キャッシュ プロパティの設定

DNS 解決のキャッシングは、以前に解決された DNS ルックアップのキャッシングを許可するシステム全体の設定です。

手順

ステップ 1 [システム（System）]（⚙）>**[構成（Configuration）]**を選択します。

ステップ 2 [DNS キャッシュ（DNS Cache）] を選択します。

ステップ 3 [DNS 解決のキャッシング（DNS Resolution Caching）] ドロップダウン リストから、次のいずれかを選択します。

- [有効化（Enabled）]：キャッシングを有効にします。
- [無効化（Disabled）]：キャッシングを無効にします。

ステップ 4 [DNS キャッシュ タイムアウト（分）（DNS Cache Timeout（in minutes））] フィールドで、非アクティブのために削除されるまで DNS エントリがメモリ内にキャッシュされる時間（分単位）を入力します。

デフォルトは 300 分（5 時間）です。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

イベント ビュー設定の設定

ダッシュボード

ダッシュボードでは、ウィジェットを使用することにより、現在のシステムステータスが一目でわかります。ウィジェットは小さな自己完結型コンポーネントであり、システムのさまざまな側面に関するインサイトを提供します。システムには、事前定義された複数のダッシュボードウィジェットが付属しています。

[カスタム分析（Custom Analysis）] ウィジェットがダッシュボードで有効になるように、Firewall Management Center を設定できます。

関連トピック

ダッシュボードについて

ダッシュボードのカスタム分析ウィジェットの有効化

[カスタム分析（Custom Analysis）] ダッシュボード ウィジェットを使用して、柔軟でユーザーによる構成が可能なクエリに基づいてイベントのビジュアル表現を作成します。

手順

ステップ 1 [システム（System）]（⚙）>**[構成（Configuration）]**を選択します。

ステップ 2 [ダッシュボード（Dashboard）] をクリックします。

ステップ 3 ユーザが [カスタム分析（Custom Analysis）] ウィジェットをダッシュボードに追加できるようにするには、[カスタム分析ウィジェットの有効化（Enable Custom Analysis Widgets）] チェックボックスをオンにします。

ステップ 4 [保存（Save）] をクリックします。

関連トピック

ダッシュボードについて

データベース

ディスク容量を管理するために、Firewall Management Center は、最も古い侵入イベント、監査レコード、セキュリティインテリジェンスデータ、URL フィルタリングデータをイベントデータベースから定期的にプルーニングします。イベントタイプごとに、Firewall Management Center がプルーニング後に保持するレコードの数を指定できます。そのタイプに設定された保持制限を超える数のレコードを含むイベントデータベースには依存しないでください。パフォーマンスを向上させるには、定期的に処理するイベント数に合わせてイベント制限を調整します。必要に応じて、プルーニングが発生したときに電子メール通知を受け取ることを選択できます。一部のイベント タイプでは、ストレージを無効にすることができます。

個々のイベントを手動で削除するには、イベントビューアを使用します。（バージョン 6.6.0 以降では、この方法で接続またはセキュリティ インテリジェンス イベントを手動で削除できないことに注意してください）。データベースを手動で消去することもできます。データの消去とストレージを参照してください。

データベース イベント数の制限の設定

始める前に

- Firewall Management Center のデータベースからイベントがプルーニングされた場合に電子メール通知を受信するには、電子メール サーバーを設定する必要があります。メール リレー ホストおよび通知アドレスの設定 （34 ページ）を参照してください。

手順

ステップ 1 [システム（System）]（⚙）>**[構成（Configuration）]**を選択します。

ステップ 2 [データベース（Database）] を選択します。

ステップ 3 各データベースについて、保存するレコードの数を入力します。

各データベースが保持できるレコード数の詳細については、データベース イベント数の制限（31 ページ）を参照してください。

ステップ 4 必要に応じて、[データ プルーニング通知のアドレス（Data Pruning Notification Address）] フィールドに、プルーニング通知を受信する電子メール アドレスを入力します。

ステップ 5 [保存（Save）] をクリックします。

データベース イベント数の制限

次の表に、Firewall Management Center ごとに保存可能な各イベントタイプのレコードの最小数と最大数を示します。

表 *2:* データベース イベント数の制限

イベントタイプ	上限	下限
侵入イベント	1,000 万（Firewall Management Center Virtual） 3,000 万（Firewall Management Center 1000、Firewall Management Center 1600、Firewall Management Center 1700） 6,000 万（Firewall Management Center 2500、Firewall Management Center 2600、Firewall Management Center 2700、FMCv 300） 3 億（Firewall Management Center4500、Firewall Management Center4600） 4 億（Firewall Management Center4700）	10,000
検出イベント	1,000 万 （Firewall Management Center 仮想） 2,000 万	0（ストレージを無効化）

イベントタイプ	上限	下限
接続イベント [セキュリティ関連のイベント（Security-Related Events）]	5,000 万（Firewall Management Center 仮想） 1 億（Firewall Management Center 1000、Firewall Management Center 1600、Firewall Management Center 1700） 3 億（Firewall Management Center 2500、Firewall Management Center 2600、Firewall Management Center 2700、FMCv 300） 10 億（Firewall Management Center4500、Firewall Management Center4600、Firewall Management Center4700） 制限は接続イベントとセキュリティ関連接続イベントの間で共有されます。設定済みの最大数の合計がこの制限を超えることはできません。	0（ストレージを無効化） **[最大接続イベント数（Maximum Connection Events）]** の値をゼロに設定すると、セキュリティ関連接続、侵入、ファイル、およびマルウェアの各イベントに関連付けられていない接続イベントは Firewall Management Center に保存されません。 **注意** **[最大接続イベント数（Maximum Connection Events）]** をゼロに設定すると、セキュリティ関連接続以外の既存の接続イベントがただちに消去されます。 この設定が最大フローレートに与える影響については、以下を参照してください。 これらの設定は、接続サマリーには影響しません。
接続の要約（集約された接続イベント）	5,000 万（Firewall Management Center 仮想） 1 億（Firewall Management Center 1000、Firewall Management Center 1600、Firewall Management Center 1700） 3 億（Firewall Management Center 2500、Firewall Management Center 2600、Firewall Management Center 2700、FMCv 300） 10 億（Firewall Management Center4500、Firewall Management Center4600、Firewall Management Center4700）	0（ストレージを無効化）
相関イベントおよびコンプライアンスの allow リスト イベント	100 万 （Firewall Management Center 仮想） 200 万（Firewall Management Center2500、Firewall Management Center2600、Firewall Management Center4500、Firewall Management Center4600、Firewall Management Center4700、FMCv 300）	1 つ

イベントタイプ	上限	下限
マルウェア イベント	1,000 万 （Firewall Management Center仮想、Firewall Management Center 1600、Firewall Management Center 1700） 2,000 万（Firewall Management Center 2500、Firewall Management Center 2600、Firewall Management Center 2700、Firewall Management Center 4500、Firewall Management Center 4600、Firewall Management Center 4700、FMCv 300）	10,000
ファイル イベント	1,000 万 （Firewall Management Center仮想、Firewall Management Center 1600、Firewall Management Center 1700） 2,000 万（Firewall Management Center 2500、Firewall Management Center 2600、Firewall Management Center 2700、Firewall Management Center 4500、Firewall Management Center 4600、Firewall Management Center 4700、FMCv 300）	0（ストレージを無効化）
ヘルス イベント	100 万	0（ストレージを無効化）
監査レコード	100,000	1 つ
修復ステータス イベント	1,000 万	1 つ
許可 リスト違反履歴	30 日間の違反履歴	1 日の履歴
ユーザー アクティビティ（ユーザー イベント）	1,000 万	1 つ
ユーザー ログイン（ユーザー履歴）	1,000 万	1 つ
侵入ルール更新のインポート ログ レコード	100 万	1 つ
トラブルシューティング ログ データベース	1,000 万	0（ストレージを無効化）

最大フローレート

Firewall Management Center ハードウェアモデルの [最大フローレート（Maximum flow rate）]（1秒あたりのフロー数）の値は、https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-736775.html?cachemode=refresh の Firewall Management Center データシートの「Platform Specifications」の項で指定されています。

プラットフォーム設定の **[最大接続イベント（Maximum Connection Events）]** 値を 0 に設定すると、(セキュリティ関連の接続イベント)、侵入、ファイル、およびマルウェアイベントに関連付けられていない接続イベントは、Firewall Management Centerハードウェアの最大フローレートにカウントされません。

このフィールドにゼロ以外の値を指定すると、すべての接続イベントが最大フローレートに対してカウントされます。

このページの他のイベントタイプは、最大フローレートにはカウントされません。

電子メール通知

次の処理を行う場合は、メール ホストを設定します。

- イベントベースのレポートの電子メール送信
- スケジュールされたタスクのステータス レポートの電子メール送信
- 変更調整レポートの電子メール送信
- データプルーニング通知の電子メール送信
- 検出イベント、影響フラグ、相関イベントアラート、侵入イベントアラート、および正常性イベントアラートに電子メールを使用します。

電子メール通知を設定する場合、システムとメール リレー ホスト間の通信に使用する暗号化方式を選択し、必要に応じて、メールサーバの認証クレデンシャルを指定できます。設定した後、接続をテストできます。

メール リレー ホストおよび通知アドレスの設定

手順

ステップ 1 [システム（System）]（⚙）>**[構成（Configuration）]**を選択します。

ステップ 2 [電子メール通知（Email Notification）] をクリックします。

ステップ 3 [メール リレー ホスト（Mail Relay Host）] フィールドで、使用するメール サーバーのホスト名または IP アドレスを入力します。入力したメール ホストはアプライアンスからのアクセスを許可している**必要があります**。

ステップ 4 [ポート番号（Port Number）] フィールドに、電子メール サーバーで使用するポート番号を入力します。

一般的なポートには次のものがあります。

- 25。暗号化を使用しない場合
- 465。SSLv3 を使用する場合
- 587。TLS を使用する場合

ステップ 5 [暗号化方式（Encryption Method）] を選択します。

- [TLS]：Transport Layer Security を使用して通信を暗号化します。
- [SSLv3]：セキュア ソケット レイヤを使用して通信を暗号化します。
- [なし（None）]：暗号化されていない通信を許可します。

（注）
アプライアンスとメール サーバーとの間の暗号化された通信では、証明書の検証は不要です。

ステップ 6 [送信元アドレス（From Address）] フィールドに、アプライアンスから送信されるメッセージの送信元電子メール アドレスとして使用する有効な電子メール アドレスを入力します。

ステップ 7 必要に応じて、メール サーバーに接続する際にユーザー名とパスワードを指定するには、[認証を使用（Use Authentication）] を選択します。[Username] フィールドにユーザー名を入力します。パスワードを [Password] フィールドに入力します。

ステップ 8 設定したメール サーバを使用してテスト メールを送信するには、[Test Mail Server Settings] をクリックします。

テストの成功または失敗を示すメッセージがボタンの横に表示されます。

ステップ 9 [保存（Save）] をクリックします。

外部データベース アクセス

サードパーティ製クライアントによるデータベースへの読み取り専用アクセスを許可するように、Firewall Management Center を設定できます。これによって、次のいずれかを使用して SQL でデータベースを照会できるようになります。

- 業界標準のレポート作成ツール（Actuate BIRT、JasperSoft iReport、Crystal Reports など）
- JDBC SSL 接続をサポートするその他のレポート作成アプリケーション（カスタム アプリケーションを含む）
- シスコが提供する RunQuery と呼ばれるコマンドライン型 Java アプリケーション（インタラクティブに実行することも、1 つのクエリの結果をカンマ区切り形式で取得することもできる）

Firewall Management Centerのシステム設定を使用して、データベースアクセスを有効にして、選択したホストにデータベースの照会を許可するアクセスリストを作成します。このアクセスリストは、アプライアンスのアクセスは制御しません。

次のツールを含むパッケージをダウンロードすることもできます。

- RunQuery（シスコが提供するデータベース クエリ ツール）
- InstallCert（アクセスしたいFirewall Management Centerから SSL 証明書を取得して受け入れるために使用できるツール）
- データベースへの接続時に使用する必要がある JDBC ドライバ

データベースアクセスを設定するためにダウンロードしたパッケージ内のツールの使用方法については、『*Cisco Secure Firewall Management Center Database Access Guide*』を参照してください。

データベースへの外部アクセスの有効化

手順

ステップ 1 [システム（System）]（⚙）>**[構成（Configuration）]**を選択します。

ステップ 2 [外部データベース アクセス（External Database Access）] をクリックします。

ステップ 3 [外部データベース アクセスの許可（Allow External Database Access）] チェックボックスをオンにします。

ステップ 4 [サーバー ホスト名（Server Hostname）] フィールドに、適切な値を入力します。サードパーティ アプリケーションの要件に応じて、この値は、Firewall Management Centerの完全修飾ドメイン名（FQDN）、IPv4 アドレス、または IPv6 アドレスにできます。

（注）
Firewall Management Center のハイアベイラビリティ設定では、アクティブピアの詳細のみを入力します。スタンバイピアの詳細を入力することはお勧めしません。

ステップ 5 [クライアント JDBC ドライバ（Client JDBC Driver）] の横にある [ダウンロード（Download）] をクリックし、ブラウザのプロンプトに従って`client.zip`パッケージをダウンロードします。

ステップ 6 1 つ以上の IP アドレスからのデータベース アクセスを追加するには、[ホストの追加（Add Hosts）] をクリックします。[アクセス リスト（Access List）] フィールドに [IP アドレス（IP Address）] フィールドが表示されます。

ステップ 7 [IP アドレス（IP Address）] フィールドに、IP アドレスまたはアドレスの範囲を入力するか、`any` を入力します。

ステップ 8 [追加（Add）] をクリックします。

ステップ 9 [保存（Save）] をクリックします。

ヒント

最後に保存されたデータベース設定に戻すには、[更新（Refresh）] をクリックします。

関連トピック

Firepower システムの IP アドレス表記法

HTTPS 証明書

Firewall Management Centerデバイスは、セキュア ソケット レイヤ（SSL）証明書によりシステムと Web ブラウザ間に暗号化チャネルを確立することができます。すべての ファイアウォールデバイスにデフォルト証明書が含まれていますが、これはグローバルレベルで既知のCAから信頼された認証局（CA）によって生成された証明書ではありません。したがって、デフォルト証明書ではなく、グローバル レベルで既知の CA または内部で信頼された CA 署名付きのカスタム証明書の使用を検討してください。

注意 Firewall Management Center は 4096 ビット HTTPS 証明書をサポートしています。Firewall Management Center で使用する証明書が 4096 ビットを超える公開サーバー キーを使用して生成されている場合、Firewall Management Center Web インターフェイスにログインできません。この問題が発生した場合は、Cisco TACにお問い合わせください。

（注） HTTPS 証明書は、Management Center の REST API ではサポートされていません。

デフォルト HTTPS サーバー証明書

アプライアンスに提供されるデフォルトサーバー証明書を使用する場合、Webインターフェイスのアクセスに有効な HTTPS クライアント証明書が必要になるようにシステムを設定しないでください。これは、デフォルトサーバー証明書が、クライアント証明書に署名する CA によって署名されないためです。

デフォルトのサーバー証明書の有効期間は、証明書がいつ生成されたかによって異なります。デフォルトのサーバー証明書の期限日を表示するには、[システム（System）]（⚙）>**[構成（Configuration）]** > [HTTPS証明書（HTTPS Certificate）] を選択します。

一部の Cisco Secure Firewall ソフトウェアのアップグレードでは、証明書を自動的に更新できることに注意してください。詳細については、該当するバージョンの『Cisco Cisco Secure FirewallRelease Notes』を参照してください。

Firewall Management Centerで、[システム（System）]（⚙）>**[構成（Configuration）]** > [HTTPS証明書（HTTPS Certificate）] ページでデフォルトの証明書を更新します。

カスタム HTTPS サーバー証明書

Firewall Management Center Web インターフェイスを使用して、システム情報と指定した ID 情報に基づいて、サーバ証明書要求を生成できます。ブラウザによって信頼されている内部認証局（CA）がインストールされている場合は、この要求を使用して証明書に署名することができます。生成された要求を認証局に送信して、サーバー証明書を要求することもできます。認証局（CA）から署名付き証明書を取得すると、その証明書をインポートできます。

HTTPS サーバー証明書の要件

HTTPS 証明書を使用して Web ブラウザと Cisco Secure Firewall アプライアンスの Web インターフェイスの間の接続を保護する場合は、インターネット X.509 公開キーインフラストラクチャ証明書および証明書失効リスト（CRL）プロファイル（RFC 5280）に準拠する証明書を使用する必要があります。サーバー証明書をアプライアンスにインポートする場合、証明書がその標準のバージョン 3（x.509 v3）に準拠していないと、システムによって証明書は拒否されます。

HTTPS サーバー証明書をインポートする前に、次のフィールドが含まれていることを確認してください。

証明書フィールド	説明
バージョン	エンコードされた証明書のバージョン。バージョン 3 を使用します。RFC 5280 のセクション 4.1.2.1 を参照してください。
Serial number	発行元 CA によって証明書に割り当てられた正の整数。発行者とシリアル番号を組み合わせて、証明書を一意に識別します。RFC 5280 のセクション 4.1.2.2 を参照してください。
シグネチャ	証明書の署名用に CA で使用されるアルゴリズムの識別子。signatureAlgorithm フィールドと一致している必要があります。RFC 5280 のセクション 4.1.2.3 を参照してください。
発行元（Issuer）	証明書を署名および発行したエンティティを識別します。RFC 5280 のセクション 4.1.2.4 を参照してください。
Validity	CA が証明書のステータスに関する情報を維持することを保証する期間。RFC 5280 のセクション 4.1.2.5 を参照してください。

証明書フィールド	説明
Subject	サブジェクトの公開キーフィールドに保存された公開キーに関連付けられているエンティティを識別します。X.500 識別名（DN）を指定する必要があります。RFC 5280 のセクション 4.1.2.6 を参照してください。
Subject Alternative Name	証明書によって保護されるドメイン名と IP アドレス。サブジェクト代替名は、RFC 5280 のセクション 4.2.1.6 で定義されています。 証明書が複数のドメインまたは IP アドレスに使用される場合は、このフィールドを使用することをお勧めします。
Subject Public Key Info	公開キーとそのアルゴリズムの識別子。RFC 5280 のセクション 4.1.2.7 を参照してください。
Authority Key Identifier	証明書の署名に使用される秘密キーに対応する公開キーを識別する手段を提供します。RFC 5280 のセクション 4.2.1.1 を参照してください。
サブジェクトキー識別子	特定の公開キーが含まれる証明書を識別する手段を提供します。RFC 5280 のセクション 4.2.1.2 を参照してください。
[キーの使用状況（Key Usage）]	証明書に含まれるキーの目的を定義します。RFC 5280 のセクション 4.2.1.3 を参照してください。
基本的制約	証明書のサブジェクトが CA で、この証明書を含む検証認証パスの最大深さかどうかを識別します。RFC 5280 のセクション 4.2.1.9 を参照してください。Cisco Secure Firewall アプライアンスで使用されるサーバー証明書の場合は、`critical CA:FALSE` を使用します。
拡張キーの用途拡張	キーの用途拡張で示されている基本的な目的に加えて、認定公開キーを使用する目的を 1 つ以上示します。RFC 5280 のセクション 4.2.1.12 を参照してください。サーバー証明書として使用できる証明書をインポートしてください。

証明書フィールド	説明
signatureAlgorithm	証明書の署名用に CA で使用されるアルゴリズムの識別子。[署名（Signature）]フィールドと一致する必要があります。RFC 5280 のセクション 4.1.1.2 を参照してください。
signatureValue	デジタル署名。RFC 5280 のセクション 4.1.1.3 を参照してください。

HTTP クライアント証明書

クライアント ブラウザの証明書チェック機能を使用して、Firepower システムの Web サーバーへのアクセスを制限できます。ユーザ証明書を有効にすると、Web サーバはユーザのブラウザ クライアントで有効なユーザ証明書が選択されていることを確認します。そのユーザ証明書は、サーバ証明書で使用されているのと同じ信頼できる認証局によって生成されている必要があります。以下の状況ではいずれの場合もブラウザは Web インターフェイスをロードできません。

- ユーザがブラウザに無効な証明書を選択する。
- ユーザがブラウザにサーバ証明書に署名した認証局が生成していない証明書を選択する。
- ユーザがブラウザにデバイスの証明書チェーンの認証局が生成していない証明書を選択する。

クライアントブラウザ証明書を確認するには、システムを設定してオンライン証明書ステータス プロトコル（OCSP）を使用するか、1 つ以上の証明書失効リスト（CRL）ファイルをロードします。OCSP を使用する場合、Web サーバは接続要求を受信すると、接続を確立する前に認証局と通信して、クライアント証明書の有効性を確認します。サーバーに 1 つ以上の CRL をロードするよう設定する場合、Web サーバーはクライアント証明書を CRL の一覧に照らして比較します。ユーザーが CRL にある失効した証明書の一覧に含まれる証明書を選択した場合、ブラウザは Web インターフェイスをロードできません。

（注） CRL を使用した証明書の確認を選択すると、システムはクライアント ブラウザ証明書、監査ログ サーバ証明書の両方の検証に同じ CRL を使用します。

現在の HTTPS サーバ証明書の表示

手順

ステップ 1 [システム（System）]（⚙）>**[構成（Configuration）]** を選択します。

ステップ 2 [HTTPS Certificate] をクリックします。

HTTPS サーバー証明書署名要求の生成

広く知られている CA または内部的に信頼できる CA によって署名されていない証明書をインストールすると、Web インターフェイスに接続しようとするとブラウザにセキュリティ警告が表示されます。

証明書署名要求（CSR）は生成元のアプライアンスまたはデバイスに対して一意です。1 つのアプライアンスの複数のデバイスに対して CSR を生成することはできません。必須のフィールドはありませんが、[CN]、[組織（Organization）]、[組織部門（Organization Unit）]、[市区町村（City/Locality）]、[州/都道府県（State/Province）]、[国/地域（Country/Region）]、および [サブジェクト代替名（Subject Alternative Name）] の値を入力することをお勧めします。

証明書要求用に生成されるキーは、ベース 64 エンコードの PEM 形式です。

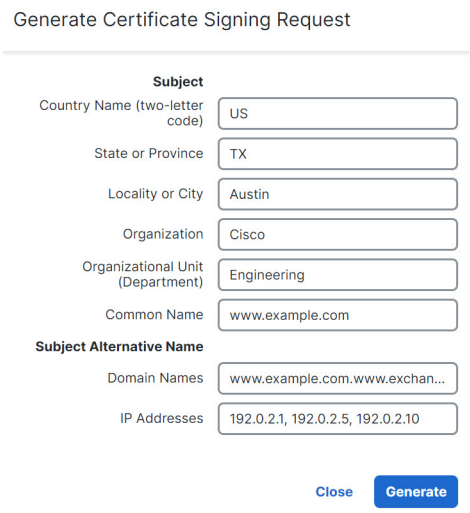
手順

ステップ 1 [システム（System）]（⚙）>**[構成（Configuration）]** を選択します。

ステップ 2 [HTTPS Certificate] をクリックします。

ステップ 3 [新規 CSR の生成（Generate New CSR）] をクリックします。

次の図は例を示しています。



ステップ 4 [国名（2 文字のコード）（Country Name (two-letter code)）] フィールドに国番号を入力します。

ステップ 5 [都道府県（State or Province）] フィールドに、都道府県名を入力します。

ステップ 6 [市区町村（Locality or City）] を入力します。

ステップ 7 [組織（Organization）] の名前を入力します。

ステップ 8 [組織単位（部署名）（Organizational Unit (Department)）] の名前を入力します。

ステップ 9 [共通名（Common Name）] フィールドに、証明書を要求するサーバーの完全修飾ドメイン名を入力します。

（注）
[共通名（Common Name）] フィールドには、証明書に表示されるとおりに、サーバーの完全修飾ドメイン名を正確に入力する必要があります。共通名と DNS ホスト名が一致していないと、アプライアンスへの接続時に警告が表示されます。

ステップ 10 複数のドメイン名または IP アドレスを保護する証明書を要求するには、[サブジェクト代替名（Subject Alternative Name）] セクションに次の情報を入力します。

a) [ドメイン名（Domain Names）]：サブジェクト代替名で保護される完全修飾ドメインとサブドメイン（存在する場合）を入力します。

b) [IP アドレス（IP Addresses）]：サブジェクト代替名で保護される IP アドレスを入力します。

ステップ 11 [生成（Generate）] をクリックします。

ステップ 12 テキスト エディタを開きます。

ステップ 13 証明書要求のテキストブロック全体（`BEGIN CERTIFICATE REQUEST` 行と `END CERTIFICATE REQUEST` 行を含む）をコピーして、空のテキスト ファイルに貼り付けます。

ステップ 14 このファイルを *servername*`.csr` として保存します。*servername* は証明書を使用するサーバーの名前です。

ステップ 15 [閉じる（Close）] をクリックします。

次のタスク

- 証明機関に証明書要求を送信します。
- 署名付き証明書を受け取ったら、Firewall Management Center にインポートします。HTTPS サーバー証明書のインポート （42 ページ）を参照してください。

HTTPS サーバー証明書のインポート

証明書を生成した署名認証局から中間 CA を信頼するように要求された場合は、証明書チェーン（証明書パス）も提供する必要があります。

クライアント証明書が必要な場合、サーバー証明書が次に示すいずれかの条件を満たしていないときに、Web インターフェイス経由でのアプライアンスへのアクセスに失敗します。

- 証明書が、クライアント証明書に署名したものと同じ CA によって署名されている。
- 証明書が、証明書チェーンの中間証明書に署名したものと同じ CA によって署名されている。

注意 Firewall Management Center は 4096 ビット HTTPS 証明書をサポートしています。Firewall Management Center で使用する証明書が 4096 ビットを超える公開サーバー キーを使用して生成されている場合、Secure Firewall Management Center Web インターフェイスにログインできません。HTTPS 証明書のバージョン 6.0.0 への更新に関する詳細は、*FirePOWER* システムリリースノート、バージョン *6.0* の「Update Management Center HTTPS Certificates to Version 6.0」を参照してください。HTTPS 証明書を生成またはインポートしていて、Firewall Management Center の Web インターフェイスにログインできない場合は、サポートまでお問い合わせください。

始める前に

- 証明書署名要求を生成します。HTTPS サーバー証明書署名要求の生成 （41 ページ）を参照してください。
- この CSR ファイルを証明書の要求先となる認証局にアップロードするか、この CSR を使用して自己署名証明書を作成します。
- 証明書がHTTPS サーバー証明書の要件 （38 ページ）で説明されている要件を満たしていることを確認します。

手順

ステップ 1 [システム（System）]（⚙）>**[構成（Configuration）]** を選択します。

ステップ 2 [HTTPS Certificate] をクリックします。

ステップ 3 [HTTPSサーバ証明書のインポート（Import HTTPS Server Certificate）] をクリックします。

（注）
暗号化された HTTPS 証明書はインポートできません。

ステップ 4 テキスト エディタでサーバー証明書を開いて、`BEGIN CERTIFICATE` の行と `END CERTIFICATE` の行を含むテキストのブロック全体をコピーします。このテキストを [サーバー証明書（Server Certificate）] フィールドに貼り付けます。

ステップ 5 **秘密キー**を指定する必要があるかどうかは、証明書署名要求の生成方法によって異なります。

- Secure Firewall Management Center Web インターフェイスを使用して証明書署名要求を生成した場合（HTTPS サーバー証明書署名要求の生成 （41 ページ）に記載）、システムにはすでに秘密キーがあるため、ここで入力する必要はありません。
- 他の方法を使用して証明書署名要求を生成した場合、ここで秘密キーを指定する必要があります。秘密キー ファイルを開いて、`BEGIN RSA PRIVATE KEY` の行と `END RSA PRIVATE KEY` の行を含むテキストのブロック全体をコピーします。このテキストを [秘密キー（Private Key）] フィールドに貼り付けます。

ステップ 6 必要な中間証明書をすべて開いて、それぞれのテキストのブロック全体をコピーして、[証明書チェーン（Certificate Chain）] フィールドに貼り付けます。ルート証明書を受け取った場合

は、ここに貼り付けます。中間証明書を受け取った場合は、ルート証明書の下に貼り付けます。どちらの場合も、BEGIN CERTIFICATE の行と END CERTIFICATE の行を含むテキストのブロック全体をコピーします。

ステップ 7 [保存（Save）] をクリックします。

有効な HTTPS クライアント証明書の強制

Firewall Management Center Webインターフェイスに接続するユーザーにユーザー証明書の提供を要求するには、次の手順を使用します。システムは、OCSP または PEM（Privacy-enhanced Electronic Mail）形式でインポートされた CRL を使用した HTTPS クライアント証明書の検証をサポートしています。

CRL を使用する場合は、失効した証明書のリストを最新の状態に保つために、CRL を更新するスケジュールタスクを作成してください。システムは、最後に更新した CRL を表示します。

（注） クライアント認証を有効にした後で Web インターフェイスにアクセスするには、ブラウザに有効なクライアント証明書が存在している（またはリーダーに CAC が挿入されている）**必要があります。**

始める前に

- 接続に使用するクライアント証明書に署名した認証局と同じ認証局で署名されたサーバー証明書をインポートします。HTTPS サーバー証明書のインポート （42 ページ）を参照してください。
- サーバー証明書チェーンをインポートします（必要な場合）。HTTPS サーバー証明書のインポート （42 ページ）を参照してください。

手順

ステップ 1 [システム（System）]（⚙） > **[構成（Configuration）]** を選択します。

ステップ 2 [HTTPS Certificate] をクリックします。

ステップ 3 [クライアント証明書の有効化（Enable Client Certificates）] を選択します。プロンプトが表示されたら、ドロップダウンリストから該当する証明書を選択します。

ステップ 4 次の 3 つのオプションがあります。

- 1 つ以上の CRL を使用してクライアント証明書を検証する場合は、[CRL のフェッチの有効化（Enable Fetching of CRL）] を選択して、手順 5 に進みます。
- OCSP を使用してクライアント証明書を検証する場合は、[OCSPの有効化（Enable OCSP）] を選択して、手順 7 に進みます。
- 失効の確認なしでクライアント証明書を承認する場合は、手順 8 に進みます。

ステップ 5 既存の CRL ファイルへの有効な URL を入力して、[CRL の追加（Add CRL）] をクリックします。最大 25 個まで CRL の追加を繰り返します。

ステップ 6 [CRL の更新（Refresh CRL）] をクリックして現在の CRL をロードするか、指定した URL から CRL をロードします。

（注）
CRL のフェッチを有効にすると、定期的に CRL を更新するスケジュール タスクが作成されます。このタスクを編集して、更新の頻度を設定します。

ステップ 7 クライアント証明書がアプライアンスにロードされた認証局によって署名されていることと、サーバー証明書がブラウザの証明書ストアにロードされている認証局によって署名されていることを確認します。（これらは同じ認証局であることが必要です）。

注意
有効化したクライアント証明書で設定を保存している場合、ブラウザの証明書ストアに有効なクライアント証明書がないと、アプライアンスへの Web サーバー アクセスがすべて無効になります。設定を保存する前に、有効なクライアント証明書がインストールされていることを確認してください。

ステップ 8 [保存（Save）] をクリックします。

関連トピック

証明書失効リストのダウンロードの設定

デフォルトの HTTPS サービス証明書の更新

ログインしているアプライアンスのサーバー証明書のみを表示できます。

手順

ステップ 1 [システム（System）]（⚙）> **[構成（Configuration）]** を選択します。

ステップ 2 [HTTPS Certificate] をクリックします。

システムがデフォルトの HTTPS サーバー証明書を使用するように設定されている場合にのみ、ボタンが表示されます。

ステップ 3 [HTTPS証明書の更新（Renew HTTPS Certificate）] をクリックします。（このオプションは、デフォルトの HTTPS サーバー証明書を使用するようにシステムが設定されている場合にのみ、証明書情報の下のディスプレイに表示されます）

ステップ 4 （オプション）[HTTPS 証明書の更新（Renew HTTPS Certificate）] ダイアログボックスで、[新しいキーの生成（Generate New Key）] を選択して証明書の新しいキーを生成します。

ステップ 5 [HTTPS 証明書の更新（Renew HTTPS Certificate）] ダイアログボックスで [保存（Save）] をクリックします。

次のタスク

[HTTPS 証明書（HTTPS Certificate）] ページに表示されている証明書の有効日が更新されていることを確認することによって証明書が更新されていることを確認できます。

情報

[システム（System）]>[設定（Configuration）] ページには、次の表に示す情報が含まれています。別途記載のない限り、フィールドはすべて読み取り専用です。

（注） 同様の情報が含まれている [ヘルプ（Help）] >[概要（About）] ページも参照してください。

フィールド	説明
名前	Firewall Management Center アプライアンスに割り当てられた説明的な名前。ホスト名をアプライアンスの名前として使用できますが、このフィールドに別の名前を入力しても、ホスト名が変更されることはありません。 この名前は、特定の統合で使用されます。たとえば、Firewall Management Center と Cisco XDR を統合すると、Security Services Exchange の **[デバイス（Device）]** リストに表示されます。 名前を変更すると、登録されているすべてのデバイスが期限切れとしてマークされ、新しい名前をデバイスにプッシュするために展開が必要になります。
製品モデル（Product Model）	アプライアンスのモデル名。
シリアル番号（Serial Number）	アプライアンスのシリアル番号。
ソフトウェア バージョン（Software Version）	アプライアンスに現在インストールされているソフトウェアのバージョン。
オペレーティング システム（Operating System）	アプライアンス上で現在実行されているオペレーティング システム。
オペレーティング システム バージョン（Operating System Version）	アプライアンス上で現在実行されているオペレーティング システムのバージョン。

フィールド	説明
IPv4 アドレス（IPv4 Address）	デフォルト管理インターフェイス（eth0）の IPv4 アドレス。IPv4 の管理が無効になっている場合は、このフィールドにそのことが示されます。
IPv6 アドレス（IPv6 Address）	デフォルト管理インターフェイス（eth0）の IPv6 アドレス。IPv6 の管理が無効になっている場合は、このフィールドに表示されます。
現在のポリシー（Current Policies）	現在展開されているシステム レベルのポリシー。ポリシーが最後に適用された後で更新されていると、ポリシー名がイタリック体で表示されます。
モデル番号（Model Number）	内部フラッシュ ドライブに保存されているアプライアンス固有のモデル番号。この番号は、トラブルシューティングで重要になる場合があります。

侵入ポリシーの設定

さまざまな侵入ポリシー設定を指定して、展開内の重要なポリシーの変更をモニターおよび追跡します。

侵入ポリシー設定の指定

侵入ポリシー設定を指定します。

手順

ステップ 1 [システム（System）]（⚙）>**[構成（Configuration）]**を選択します。

ステップ 2 [侵入ポリシー設定（Intrusion Policy Preferences）] をクリックします。

ステップ 3 次の選択肢があります。

- [ポリシーの変更に関するコメント（Comments on policy change）]：ユーザーが侵入ポリシーを変更するときに、コメント機能を使用してポリシー関連の変更を追跡するには、このチェックボックスをオンにします。ポリシー変更のコメントが有効にされていると、管理者はコメントにアクセスして、導入で重要なポリシーが変更された理由を素早く評価できます。

  ポリシーの変更に関するコメントを有効にした場合、コメントをオプションまたは必須に設定できます。Firewall Management Centerは、ポリシーに対する新しい変更が保存されるたびに、ユーザーにコメントを入力するようプロンプトを出します。

- [侵入ポリシーの変更を監査ログに書き込む（Write changes in Intrusion Policy to audit log）]：侵入ポリシーの変更を監査ログに記録するには、このチェックボックスをオンにします。このオプションは、デフォルトで有効です。
- [削除されたSnort 3ルールのユーザーオーバーライドの保持（Retain user overrides for deleted Snort 3 rules）]：LSP 更新中に「オーバーライドされた」システム定義ルールの変更に関する通知を受け取るには、このチェックボックスをオンにします。オンにすると、LSP 更新の一部として追加される新しい置換ルールのルールオーバーライドが保持されます。通知を表示するには、Firewall Management Center メニューバーで、**[通知（Notification）]** > **[タスク（Tasks）]** をクリックします。このオプションは、デフォルトで有効です。
- **[Talos 脅威ハンティング テレメトリ（Talos Threat Hunting Telemetry）]**：Cisco Talos が脅威ハンティングを実行し、重要なセキュリティインテリジェンスを収集することを可能にするには、このチェックボックスをオンにします。オンにすると、特別な一連の脅威ハンティングルールがグローバル侵入ポリシーに追加されます。脅威ハンティングルールは通常の IPS ルールと同様に処理されますが、Talos 脅威ハンティングルールが生成するイベントは、Firewall Management Center のイベントテーブルには表示されません。代わりに、イベントが、分析のためにテレメトリとして Talos に送信されます。このオプションは、デフォルトで有効です。

  （注）
  - 脅威ハンティングルールイベントは、Cisco Success Network オプションが有効になっている場合にのみ Talos に転送されます。Cisco Success Network の詳細については、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　（9 ページ）を参照してください。
  - 自分の Security Cloud Control アカウントを使用して Firewall Management Center をクラウドテナントに登録し、直接接続でファイアウォールイベントを Cisco Security Cloud に送信する場合、脅威ハンティングルールのイベントを Talos に転送するため、Security Cloud Control アカウントには セキュリティ分析とロギング ライセンスが必要です。

言語

[言語（Language）] ページを使用して、Web インターフェイス用に異なる言語を指定できます。

Web インターフェイスの言語の設定

ここで指定した言語は、すべてのユーザーの Web インターフェイスに使用されます。次の中から選択できます。

- 英語

- フランス語
- 中国語（簡体字）
- 中国語（繁体字）
- 日本語
- 韓国語

手順

ステップ 1 [システム（System）]（⚙）>**[構成（Configuration）]**を選択します。
ステップ 2 [言語（Language）] をクリックします。
ステップ 3 使用する言語を選択します。
ステップ 4 [保存（Save）] をクリックします。

ログイン バナー

[ログイン バナー（Login Banner）] ページを使用して、セキュリティ アプライアンスまたは共有ポリシーのセッション バナー、ログイン バナー、カスタム メッセージ バナーを指定できます。

カスタムログインバナーを作成するには、ASCII 文字と改行を使用できます。タブによるスペース設定は維持されません。ログイン バナーが大きすぎる場合や、エラーの原因となる場合、システムがバナーを表示しようとすると、TelnetまたはSSHセッションが失敗することがあります。

ログイン バナーのカスタマイズ

手順

ステップ 1 [システム（System）]（⚙）>**[構成（Configuration）]**を選択します。
ステップ 2 [ログイン バナー（Login Banner）] を選択します。
ステップ 3 [カスタム ログイン バナー（Custom Login Banner）] フィールドに、使用するログイン バナー テキストを入力します。
ステップ 4 [保存（Save）] をクリックします。

管理インターフェイス

セットアップの完了後、管理ネットワーク設定を変更することができます。これには、Firewall Management Center での管理インターフェイス、ホスト名、検索ドメイン、DNS サーバー、HTTP プロキシの追加が含まれます。

Firewall Management Center 管理インターフェイスについて

デフォルトでは、Firewall Management Center はすべてのデバイスを 1 つの管理インターフェイス上で制御します。また、初期設定や、管理者として Firewall Management Center にログインする際にも管理インターフェイスで行うことができます。管理インターフェイスは、スマートライセンスサーバーとの通信、更新プログラムのダウンロード、その他の管理機能の実行にも使用します。

デバイス管理インターフェイスについては、Cisco Secure Firewall Management Center デバイス構成ガイドの「*About Device Management Interfaces*」を参照してください。

デバイス管理について

Firewall Management Center がデバイスを管理するときは、デバイスとの間に、双方向の SSL 暗号化通信チャネルをセットアップします。Firewall Management Center はこのチャネルを使用して、そのデバイスへのネットワーク トラフィックの分析および管理の方法に関する情報をそのデバイスに送信します。そのデバイスはトラフィックを評価すると、イベントを生成し、同じチャネルを使用してそれらのイベントを Firewall Management Center に送信します。

Firewall Management Center を使用してデバイスを管理すると、以下の利点があります。

- すべてのデバイスのポリシーを一箇所から設定できるため、設定の変更が容易になります。
- さまざまなタイプのソフトウェア アップデートをデバイスにインストールできます。
- 正常性ポリシーを管理対象デバイスに適用して、Firewall Management Center からデバイスのヘルス ステータスをモニターできます。

（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。デバイス設定およびその他のサポートされていない機能に関連するこのガイドの章と手順は、プライマリマネージャが Security Cloud Control のデバイスには適用されません。

Firewall Management Center は、侵入イベント、ネットワーク検出情報、およびデバイスのパフォーマンスデータを集約して相互に関連付けます。そのため、ユーザはデバイスが相互の関

連でレポートする情報をモニタして、ネットワーク上で行われている全体的なアクティビティを評価することができます。

Firewall Management Center を使用することで、デバイス動作のほぼすべての側面を管理できます。

（注） Firewall Management Center は、http://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html で入手可能な互換性マトリックスで指定されている特定の以前のリリースを実行しているデバイスを管理できますが、これらの以前のリリースのデバイスでは、最新バージョンの Firewall Threat Defense ソフトウェアが必要な新しい機能は利用できません。一部の Firewall Management Center 機能は、以前のバージョンで使用できる場合があります。

管理接続

Firewall Management Center 情報を使用してデバイスを設定し、デバイスを Firewall Management Center に追加した後に、デバイスまたは Firewall Management Center のいずれかで管理接続を確立できます。初期設定に応じて、以下のようになります。

- デバイスまたは Firewall Management Center のいずれかから開始できる。
- デバイスのみが開始できる。
- Firewall Management Center のみが開始できる。

初期化は常に Firewall Management Center の eth0 またはデバイスの最も番号が小さい管理インターフェイスから始まります。接続が確立されていない場合は、追加の管理インターフェースが試行されます。Firewall Management Center の複数の管理インターフェイスにより、個別のネットワークに接続したり、管理トラフィックとイベントトラフィックを分離したりできます。ただし、イニシエータは、ルーティングテーブルに基づいて最適なインターフェイスを選択しません。

管理接続が安定しており、過度なパケット損失がなく、少なくとも 5 Mbps のスループットがあることを確認します。デフォルトでは、管理接続は TCP ポート 8305 を使用します（このポートは設定可能です）。デバイスと Firewall Management Center の間に別の Firewall Threat Defense を配置する場合は、管理の中断を防ぐために、プレフィルタポリシーを適用して管理トラフィックをディープインスペクションから除外してください。

（注） 管理接続は、それ自身とデバイスの間の安全な TLS-1.3 暗号化通信チャネルです。セキュリティ上の理由から、サイト間 VPN などの追加の暗号化トンネル経由でこのトラフィックを実行する必要はありません。たとえば、VPN がダウンすると、管理接続が失われるため、シンプルな管理パスをお勧めします。

Firewall Management Center 上の管理インターフェイス

Firewall Management Center では、初期セットアップ、管理者の HTTP アクセス、デバイスの管理、ならびにその他の管理機能（ライセンス管理や更新など）に、eth0 インターフェイスが使用されます。

追加の管理インターフェイスを設定することもできます。Firewall Management Center がさまざまなネットワーク上で多数のデバイスを管理している場合、管理インターフェイスをさらに追加することで、スループットとパフォーマンスの向上につながります。これらの管理インターフェイスをその他すべての管理機能に使用することもできます。管理インターフェイスごとに、対応する機能を限定することをお勧めします。たとえば、ある特定の管理インターフェイスを HTTP 管理者アクセス用に使用し、別の管理インターフェイスをデバイスの管理に使用するなどです。

デバイス管理用に、管理インターフェイスには 2 つの別個のトラフィック チャネルがあります。管理トラフィック チャネルはすべての内部トラフィック（デバイス管理に固有のデバイス間トラフィックなど）を伝送し、イベント トラフィック チャネルはすべてイベント トラフィック（Web イベントなど）を伝送します。オプションで、Firewall Management Center 上にイベントを処理するためのイベント専用インターフェイスを別個に設定することもできます。設定できるイベント専用インターフェイスは 1 つだけです。管理トラフィックチャネルの管理インターフェイスも常に必要です。イベント トラフィックは大量の帯域幅を使用する可能性があるので、管理トラフィックからイベント トラフィックを分離することで、Firewall Management Center のパフォーマンスを向上させることができます。たとえば、10 GigabitEthernet インターフェイスをイベント インターフェイスとして割り当て、可能なら、1 GigabitEthernet インターフェイスを管理用に使用します。たとえば、イベント専用インターフェイスは完全にセキュアなプライベート ネットワーク上に設定し、通常の管理インターフェイスはインターネットにアクセスできるネットワーク上で使用することをお勧めします。同じネットワークで管理インターフェイスとイベントインターフェイスの両方を使用することもできますが、他のデバイスから Management Center へのルーティングの問題など、潜在的なルーティングの問題を回避するために、各インターフェイスを個別のネットワークに配置することをお勧めします。管理対象デバイスは、管理トラフィックを Firewall Management Center の管理インターフェイスに送信し、イベントトラフィックを Firewall Management Center のイベント専用インターフェイスに送信します。管理対象デバイスがイベント専用インターフェイスに到達できない場合、フォールバックして管理インターフェイスにイベントを送信します。ただし、イベント専用インターフェイスを介して管理接続を確立することはできません。

Firewall Management Center からの管理接続の初期化は、常に eth0 から試行され、その後に他のインターフェイスが順番に試行されます。ルーティングテーブルは、最適なインターフェイスの決定には使用されません。

（注） すべての管理インターフェイスは、アクセスリスト設定による制御に従って HTTP 管理者アクセスをサポートしています（アクセス リストの設定 （13 ページ））。逆に、インターフェイスを HTTP アクセスのみに制限することはできません。管理インターフェイスでは、常にデバイス管理がサポートされます（管理トラフィック、イベントトラフィック、またはその両方）。

（注） eth0 インターフェイスのみが DHCP IP アドレスをサポートします。他の管理インターフェイスはスタティック IP アドレスのみをサポートします。

Firewall Management Center モデルごとの管理インターフェイスサポート

管理インターフェイスの場所については、ご使用のモデルのハードウェアインストレーションガイドを参照してください。

各 Firewall Management Center モデルでサポートされる管理インターフェイスについては、以下の表を参照してください。

表 *3 : Firewall Management Center* でサポートされる管理インターフェイス

モデル	管理インターフェイス
MC1000	eth0（デフォルト） eth1
MC2500、MC4500	eth0（デフォルト） eth1 eth2 eth3
MC1600、MC2600、MC4600	eth0（デフォルト） eth1 eth2 eth3 CIMC（Lights-Out Management でのみサポート）
FMC1700、FMC2700、FMC4700	eth0（デフォルト） eth1 eth2 eth3 CIMC（Lights-Out Management でのみサポート）
Firewall Management Center Virtual	eth0（デフォルト）

Firewall Management Center 管理インターフェイス上のネットワークルート

管理インターフェイス（イベント専用インターフェイスを含む）は、リモートネットワークに到達するためのスタティックルートのみをサポートしています。Firewall Management Centerをセットアップすると、セットアッププロセスにより、指定したゲートウェイ IP アドレスへのデフォルトルートが作成されます。このルートを削除することはできません。また、このルートで変更できるのはゲートウェイ アドレスのみです。

一部のプラットフォームでは、複数の管理インターフェイスを設定できます。デフォルトルートには出力インターフェイスが含まれていないため、選択されるインターフェイスは、指定したゲートウェイアドレスと、ゲートウェイが属するインターフェイスのネットワークによって異なります。デフォルトネットワーク上に複数のインターフェイスがある場合、デバイスは出力インターフェイスとして番号の小さいインターフェイスを使用します。

リモートネットワークにアクセスするには、管理インターフェイスごとに1つ以上のスタティックルートを使用することをお勧めします。他のデバイスから Firewall Management Center へのルーティングの問題など、潜在的なルーティングの問題を回避するために、各インターフェイスを個別のネットワークに配置することをお勧めします。

（注） 管理接続に使用されるインターフェイスは、ルーティングテーブルによって決定されません。接続は常に最初にeth0を使用して試行され、その後、管理対象デバイスに到達するまで、後続のインターフェイスが順番に試行されます。

NAT 環境

ネットワーク アドレス変換（NAT）とは、ルータを介したネットワーク トラフィックの送受信方式であり、送信元または宛先 IP アドレスの再割り当てが行われます。NAT の最も一般的な用途は、プライベートネットワークがインターネットと通信できるようにすることです。スタティック NAT は 1:1 変換を実行し、デバイスとの Firewall Management Center 通信に支障はありませんが、ポート アドレス変換（PAT）がより一般的です。PAT では、単一のパブリック IP アドレスと一意のポートを使用してパブリック ネットワークにアクセスできます。これらのポートは必要に応じて動的に割り当てられるため、PATルータの背後にあるデバイスへの接続は開始できません。

通常は、ルーティングと認証の両方の目的で両方のIPアドレス（登録キー付き）が必要です。デバイスを追加するときに、Firewall Management Center がデバイスの IP アドレスを指定し、デバイスが Firewall Management Center の IP アドレスを指定します。ただし、IP アドレスの 1 つのみがわかっている場合（ルーティング目的の最小要件）は、最初の通信用に信頼を確立して正しい登録キーを検索するために、接続の両側に一意の NAT ID を指定する必要もあります。Firewall Management Centerおよびデバイスでは、初期登録の認証と承認を行うために、登録キーおよびNAT ID（IP アドレスではなく）を使用します。

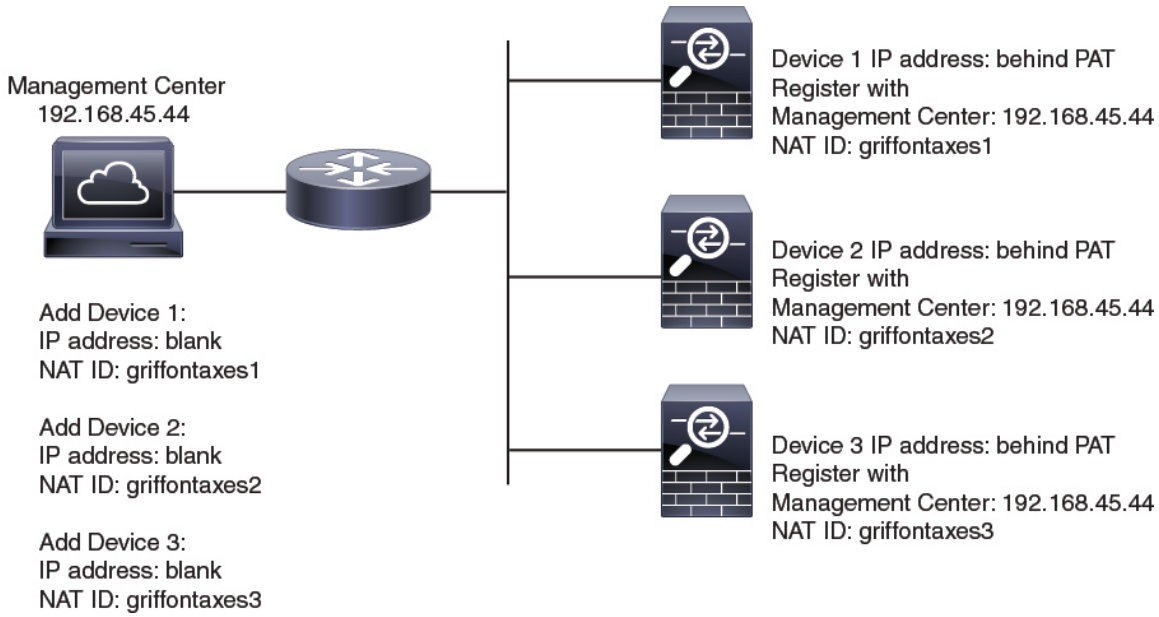
たとえば、デバイスを Firewall Management Center に追加したときにデバイスの IP アドレスがわからない場合（たとえばデバイスが PAT ルータの背後にある場合）は、NAT ID と登録キーのみを Firewall Management Center に指定します。IP アドレスは空白のままにします。デバイス上で、Firewall Management Center の IP アドレス、同じ NAT ID、および同じ登録キーを指定

します。デバイスが Firewall Management Center の IP アドレスに登録されます。この時点で、Firewall Management Center は IP アドレスの代わりに NAT ID を使用してデバイスを認証します。

NAT 環境では NAT ID を使用するのが最も一般的ですが、NAT ID を使用することで、多数のデバイスを簡単に Firewall Management Center に追加することができます。Firewall Management Center で、追加するデバイスごとに IP アドレスは空白のままにして一意の NAT ID を指定し、次に各デバイスで、Firewall Management Center の IP アドレスと NAT ID の両方を指定します。注：NAT ID はデバイスごとに一意でなければなりません。

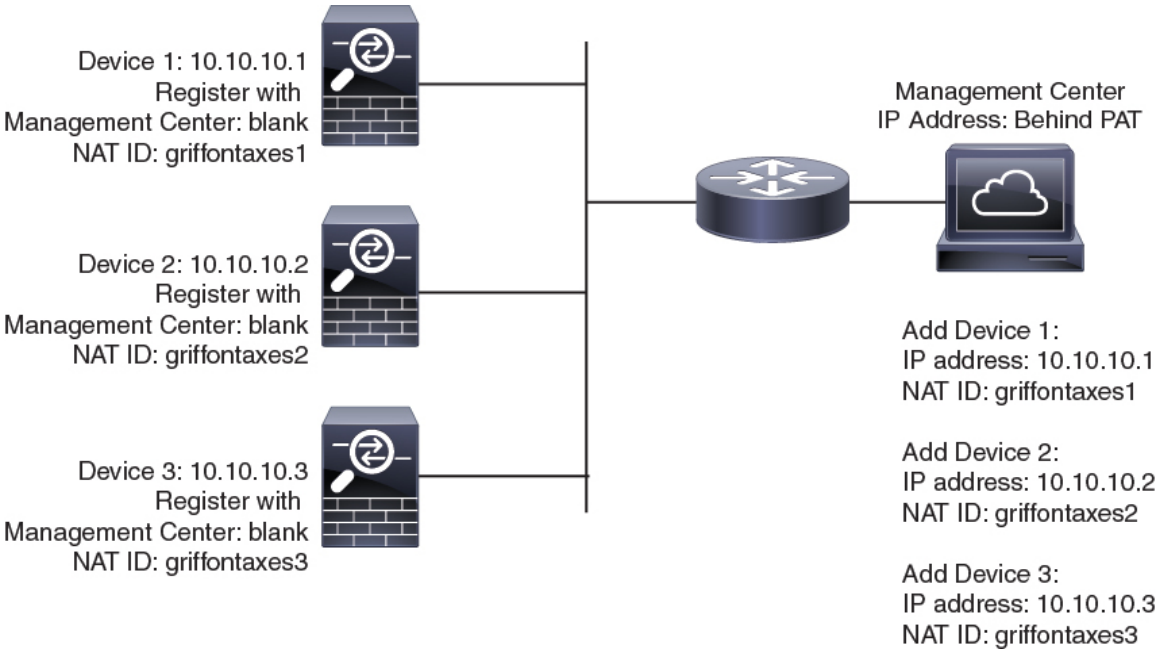
次の例に、PAT IP アドレスの背後にある 3 台のデバイスを示します。この場合、Firewall Management Center とデバイスの両方でデバイスごとに一意の NAT ID を指定し、デバイス上の Firewall Management Center の IP アドレスを指定します。

図 *5 : PAT* の背後にある管理対象デバイスの *NAT ID*



次の例に、PAT IP アドレスの背後にある Firewall Management Center を示します。この場合、Firewall Management Center とデバイスの両方でデバイスごとに一意の NAT ID を指定し、Firewall Management Center 上のデバイスの IP アドレスを指定します。

図 *6 : PAT* の背後にある *FMC* の *NAT ID*

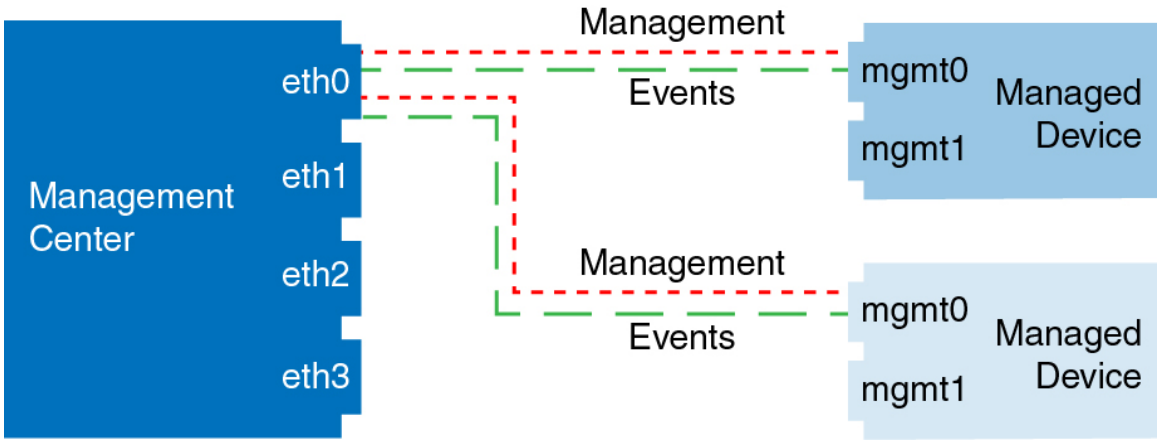


管理およびイベント トラフィック チャネルの例

（注） 管理用のデータインターフェイスを Firewall Threat Defense で使用する場合は、そのデバイスに個別の管理インターフェイスとイベントインターフェイスを使用することはできません。

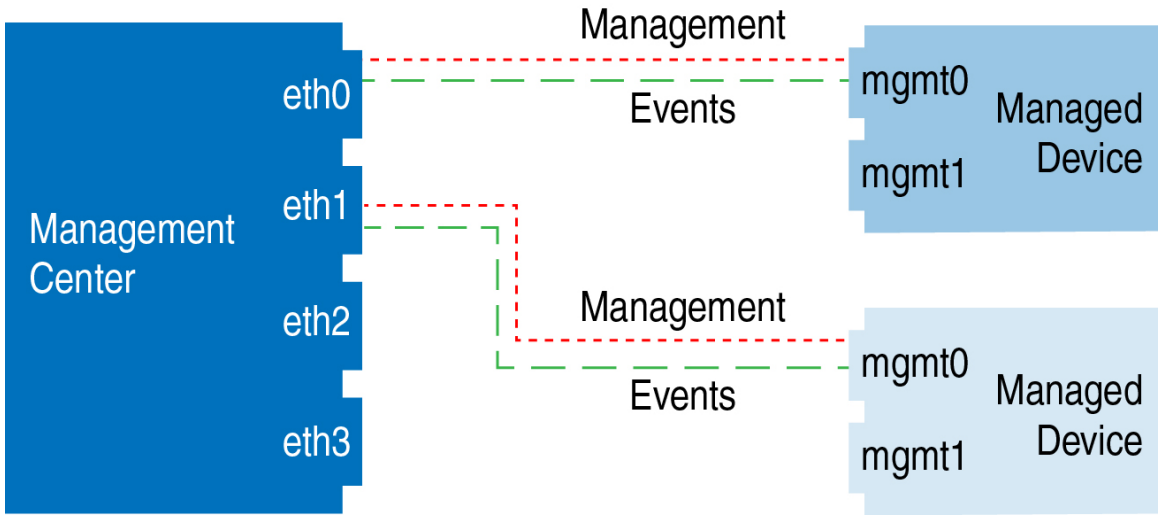
以下に、Firewall Management Center と管理対象デバイスでデフォルト管理インターフェイスのみを使用する例を示します。

図 *7 : Secure Firewall Management Center* 上で単一の管理インターフェイスを使用する場合



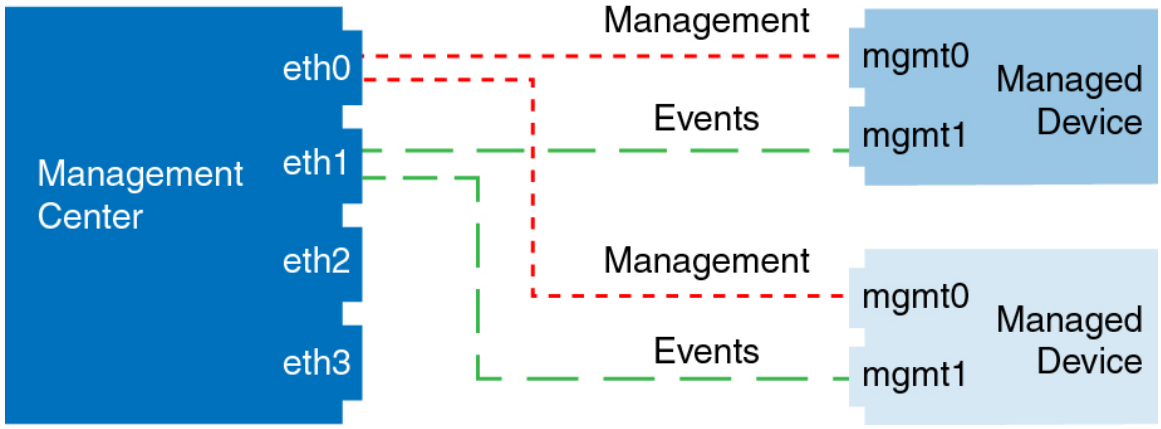
以下に、Firewall Management Center でデバイスごとに別個の管理インターフェイスを使用する例を示します。この場合、各管理対象デバイスが 1 つの管理インターフェイスを使用します。

図 *8 : Secure Firewall Management Center* の複数の管理インターフェイス



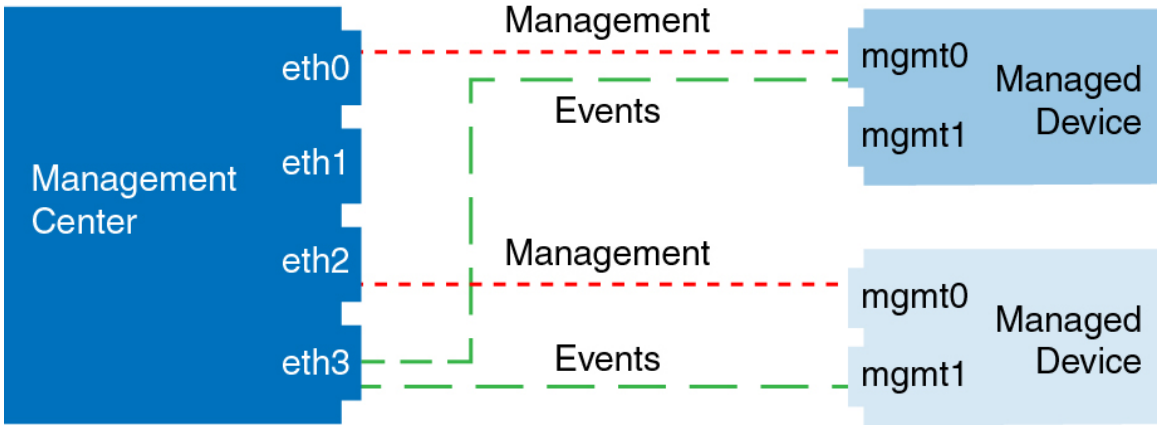
以下に、個別のイベント インターフェイスを使用する Firewall Management Center と管理対象デバイスの例を示します。

図 *9 : Secure Firewall Management Center*上の個別のイベント インターフェイスと管理対象デバイスを使用する場合



以下に、Firewall Management Center 上で複数の管理インターフェイスと個別のイベント インターフェイスが混在し、個別のイベントインターフェイスを使用する管理対象デバイスと単一の管理インターフェイスを使用する管理対象デバイスが混在する例を示します。

図 *10*：管理インターフェイスとイベント インターフェイスを混在させて使用する場合



Firewall Management Center 管理インターフェイスの変更

Firewall Management Center で管理インターフェイスの設定を変更します。オプションとして追加の管理インターフェイスを有効にしたり、イベントのみのインターフェイスを設定したりできます。

注意 接続されている管理インターフェイスを変更する場合は十分にご注意ください。設定エラーのために再接続できない場合は、Firewall Management Center コンソール ポートにアクセスして、Linux シェルでネットワーク設定を再設定する必要があります。この操作では、Cisco TAC に連絡する必要があります。

Firewall Management Center の IP アドレスを変更する場合は、Cisco Secure Firewall Management Center デバイス構成ガイド で『*Edit the Firewall Management Center IP Address or Hostname on the Device*』を参照してください。Firewall Management Center の IP アドレスまたはホスト名を変更する場合は、設定が一致するようにデバイス CLI で値を変更する必要があります。ほとんどの場合、管理接続はデバイスの Firewall Management Center IP アドレスまたはホスト名を変更せずに再確立されますが、少なくともデバイスを Firewall Management Center に追加して NAT ID のみを指定した場合は、接続が再確立されるようにするために、このタスクを実行する必要があります。他の場合でも、Firewall Management Center IP アドレスまたはホスト名を最新の状態に維持して、ネットワークの復元力を高めることを推奨します。

高可用性構成では、登録されたデバイスの管理 IP アドレスをデバイスの CLI または Firewall Management Center から変更した場合、高可用性同期後も、セカンダリ Firewall Management Center には変更が反映されません。セカンダリ Firewall Management Center も更新されるようにするには、2 つの Firewall Management Center の間でロールを切り替えて、セカンダリ Firewall Management Center をアクティブユニットにします。現在アクティブな Firewall Management Center の [デバイス管理（Device Management）] ページで、登録されているデバイスの管理 IP アドレスを変更します。

高可用性構成で 1 台のピア Firewall Management Center の管理 IP アドレスを変更した場合、リモートピアには、高可用性同期後も変更が反映されません。リモートピア Firewall Management Center も更新されるようにするには、リモートピア Firewall Management Center にログインし、[統合（Integration）] > [その他の統合（Other Integrations）] > [高可用性（High Availability）] > [ピアマネージャ（Peer Manager）] に移動し、ピアマネージャの IP アドレスを手動で更新する必要があります。 > > > 手順の詳細については、高可用性ペアの Firewall Management Center の IP アドレスの変更 を参照してください。

始める前に

- デバイス管理の仕組みについては、Cisco Secure Firewall Management Center デバイス構成ガイドで『*About Device Management Interfaces*』を参照してください。
- プロキシを使用する場合：
  - NT LAN Manager（NTLM）認証を使用するプロキシはサポートされません。
  - スマートライセンスを使用しているか、または使用する予定がある場合は、プロキシの FQDN は 64 文字以内にする必要があります。

手順

ステップ 1 [システム（System）]（⚙）>**[設定（Configuration）]**>**[管理インターフェイス（Management Interfaces）]**を選択します。

ステップ 2 [インターフェイス（Interfaces）]エリアで、設定するインターフェイスの横にある [編集（Edit）] をクリックします。

このセクションでは、利用可能なすべてのインターフェイスがリストされます。インターフェイスをさらに追加することはできません。

それぞれの管理インターフェイスに対して、以下のオプションを設定できます。

- [有効にする（Enabled）]：管理インターフェイスを有効にします。デフォルト eth0 管理インターフェイスを無効にしないでください。eth0 インターフェイスを必要とするプロセスもあります。
- [チャネル（Channels）]：[管理トラフィック（Management Traffic）] が有効になっているインターフェイスが常に少なくとも 1 つ必要です。必要に応じて、イベント専用インターフェイスを設定できます。Firewall Management Center で設定できるイベントインターフェイスは 1 つだけです。これを設定するには、[管理トラフィック（Management Traffic）] チェックボックスをオフにして、[イベント トラフィック（Event Traffic）] チェックボックスをオンのままにしておきます。必要に応じて、管理インターフェイスの [イベントトラフィック（Event Traffic）] を無効にすることができます。いずれの場合も、デバイスは、イベントのみのインターフェイスにイベントを送信しようとします。そのインターフェイスがダウンしていた場合は、イベントチャンネルが無効になっていても、管理インターフェイス上でイベントを送信します。インターフェイス上でイベントチャネルと管理チャンネルの両方を無効にすることはできません。

- [モード（Mode）]：リンク モードを指定します。ギガビット イーサネット インターフェイスでは、自動ネゴシエーションの値を変更しても反映されないことに注意してください。
- [MDI/MDIX]：[自動-MDIX（Auto-MDIX）] を設定します。
- [MTU]：1280 ～ 1500 の最大伝送ユニット（MTU）を設定します。デフォルトは 1500 です。
- [IPv4 設定（IPv4 Configuration）]：IPv4 IP アドレスを設定します。次のどちらかを選択します。
  - [スタティック（Static）]：**IPv4 の管理 IP アドレス** と**ネットマスク**を手動で入力します。
  - [DHCP]：DHCP を使用するインターフェイスを設定します（eth0 のみ）。

    DHCP を使用する場合は、割り当てられたアドレスが変更されないように、DHCP 予約を使用する必要があります。DHCP アドレスが変更されると、Firewall Management Center ネットワーク設定が同期しなくなるため、デバイスの登録は失敗します。DHCP アドレスの変更を回復するには、Firewall Management Center に接続し（ホスト名または新しい IP アドレスを使用）、[システム（System）]（⚙）>**[設定（Configuration）]** > **[管理インターフェイス（Management Interfaces）]** の順にクリックしてネットワークをリセットします。
  - [無効（Disabled）]：無効 IPv4。IPv4 と IPv6 の両方を無効に**しないでください**。
- [IPv6 設定（IPv6 Configuration）]：IPv6 IP アドレスを設定します。次のどちらかを選択します。
  - [スタティック（Static）]：**IPv6 の管理 IP アドレス**と **IPv6 のプレフィックス長**を手動で入力します。
  - [DHCP]：DHCPv6 を使用するインターフェイスを設定します（eth0 のみ）。
  - [ルータ割当て（Router Assigned）]：ステートレス自動設定を有効にします。
  - [無効（Disabled）]：IPv6 を無効にします。IPv4 と IPv6 の両方を無効に**しないでください**。
  - [IPv6 DAD]：IPv6 を有効にするときに [重複アドレス検出（DAD）] を有効または無効にします。DAD を使用することによってサービス拒否攻撃の可能性が拡大するため、DAD は無効にすることができます。この設定を無効にした場合は、すでに割り当てられているアドレスがこのインターフェイスで使用されていないことを手動で確認する必要があります。

ステップ 3 [ルート（Routes）]エリアで、静的ルートを[編集（Edit）]（✎）をクリックして編集するか、または [追加（Add）]（＋）をクリックして追加します。

ルート テーブルを表示するには、[表示（View）]（👁）アイコンをクリックします。

追加の各インターフェイスがリモート ネットワークに到達するには、スタティック ルートが必要です。新しいルートが必要な場合については、Firewall Management Center 管理インターフェイス上のネットワークルート （54 ページ）を参照してください。

（注）
デフォルト ルートでは、ゲートウェイ IP アドレスのみを変更できます。出力インターフェイスは、指定したゲートウェイをインターフェイスのネットワークに照合することで自動的に選択されます。

次の設定をスタティック ルートに対して設定できます。

- [宛先（Destination）]：ルートを作成する宛先ネットワークのアドレスを設定します。
- [ネットマスク（Netmask）] または [プレフィックス長（Prefix Length）]：ネットワークのネットマスク（IPv4）またはプレフィックス長（IPv6）を設定します。
- [インターフェイス（Interface）]：出力管理インターフェイスを設定します。
- [ゲートウェイ（Gateway）]：ゲートウェイ IP アドレスを設定します。

ステップ 4 [共有設定（Shared Settings）] エリアで、すべてのインターフェイスで共有されているネットワーク パラメータを設定します。

（注）
eth0 インターフェイスで [DHCP] を選択すると、DHCP サーバーから取得する共有設定の一部を手動で指定することができなくなります。

以下の共有設定を行うことができます。

- [ホスト名（Hostname）]：Firewall Management Center ホスト名を設定します。ホスト名は最大 64 文字を使用でき、アルファベットまたは数字で開始および終了する必要があります。使用できるのはアルファベット、数字、ハイフンのみです。ホスト名を変更する場合、syslog メッセージに反映される新しいホスト名を使用するには、Firewall Management Center を再起動します。再起動するまでは、新しいホスト名が Syslog メッセージに反映されません。
- [ドメイン（Domains）]：カンマで区切られた、Firewall Management Center の検索ドメインを 1 つ以上設定します。これらのドメインは、コマンド（**ping system** など）に完全修飾ドメイン名を指定しない場合にホスト名に追加されます。ドメインは、管理インターフェイスまたは管理インターフェイスを経由するコマンドでのみ、使用されます。
- [プライマリ DNS サーバー（Primary DNS Server）]、[セカンダリ DNS サーバー（Secondary DNS Server）]、[テリタリ DNS サーバー（Tertiary DNS Server）]：DNS サーバーが優先順で使用されるよう設定します。
- [リモート管理ポート（Remote Management Port）]：管理対象デバイスとの通信用のリモート管理ポートを設定します。Firewall Management Center および管理対象デバイスは、双方向の SSL 暗号化通信チャネル（デフォルトではポート 8305）を使用して通信します。

（注）

シスコは、リモート管理ポートをデフォルト設定のままにしておくことを**強く**推奨していますが、管理ポートがネットワーク上の他の通信と競合する場合は、別のポートを選択できます。管理ポートを変更する場合は、導入内の相互に通信する必要がある**すべての**デバイスの管理ポートを変更する必要があります。

ステップ 5 [ICMPv6] 領域で、ICMPv6 の設定を行います。

- [エコー応答パケットの送信を許可する（Allow Sending Echo Reply Packets）]：エコー応答パケットを有効または無効にします。これらのパケットを無効にすることで、サービス拒否攻撃の可能性から保護します。エコー応答パケットを無効にすると、Firewall Management Center の管理インターフェイスにテスト目的で IPv6 ping を使用できなくなります。
- [宛先到達不能パケットの送信を許可する（Allow Sending Destination Unreachable Packets）]：宛先到達不能パケットを有効または無効にします。これらのパケットを無効にすることで、サービス拒否攻撃の可能性から保護します。

ステップ 6 [プロキシ（Proxy）] エリアで、HTTP プロキシ設定をします。

Firewall Management Center は、ポート TCP/443（HTTPS）および TCP/80（HTTP）でインターネットに直接接続するように構成されています。HTTP ダイジェスト経由で認証できるプロキシ サーバーを使用できます。

このトピックの前提条件のプロキシの要件を参照してください。

a) [有効（Enabled）] チェックボックスをオンにします。
b) [HTTP プロキシ（HTTP Proxy）] フィールドに、プロキシ サーバーの IP アドレスまたは完全修飾ドメイン名を入力します。

   このトピックの前提条件の要件を参照してください。

c) [ポート（Port）] フィールドに、ポート番号を入力します。
d) [プロキシ認証の使用（Use Proxy Authentication）] を選択してから [ユーザー名（User Name）] と [パスワード（Password）] を入力して、認証資格情報を設定します。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 Firewall Management Center の IP アドレスを変更する場合は、Cisco Secure Firewall Management Center デバイス構成ガイド で『*Edit the Firewall Management Center IP Address or Hostname on the Device*』を参照してください。

Firewall Management Center の IP アドレスまたはホスト名を変更する場合は、設定が一致するようにデバイス CLI で値を変更する必要があります。ほとんどの場合、管理接続はデバイスの Firewall Management Center IP アドレスまたはホスト名を変更せずに再確立されますが、少なくともデバイスを Firewall Management Center に追加して NAT ID のみを指定した場合は、接続が再確立されるようにするために、このタスクを実行する必要があります。他の場合でも、Firewall Management Center IP アドレスまたはホスト名を最新の状態に維持して、ネットワークの復元力を高めることを推奨します。

Management Center と Threat Defense の両 IP アドレスの変更

Firewall Management Center と Firewall Threat Defense の IP アドレスを新しいネットワークに移動する場合は、両方を変更することをお勧めします。

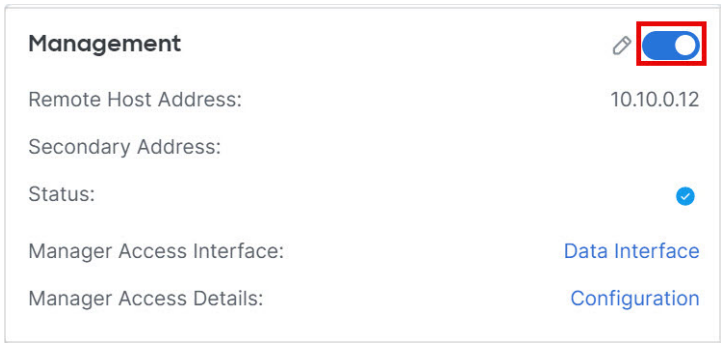
手順

ステップ 1 管理接続を無効にします。

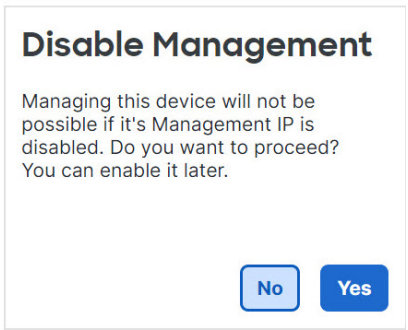
高可用性ペアまたはクラスタの場合は、すべてのユニットでこれらの CLI 手順を実行します。

a) **[デバイス（Devices）] > [デバイス管理（Device Management）]**を選択します。
b) デバイスの横にある [編集（Edit）]（ ） をクリックします。
c) [Device] をクリックし、[Management] 領域を表示します。
d) スライダをクリックして管理を一時的に無効にすることで、（ ） を無効化します。

図 *11* : 管理を無効にする



管理の無効化を続行するように求められます。 [Yes] をクリックします。



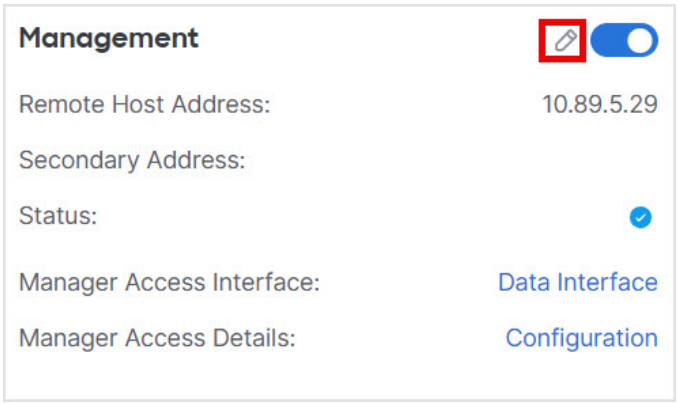
ステップ 2 Firewall Management Center 内のデバイスの IP アドレスを新しいデバイスの IP アドレスに変更します。

デバイスの IP アドレスは後で変更します。

高可用性ペアまたはクラスタの場合は、すべてのユニットでこれらの CLI 手順を実行します。

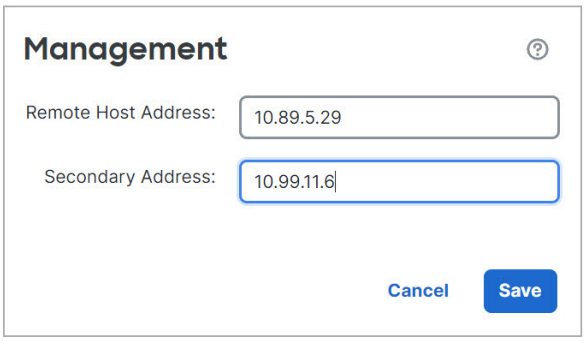
a) **[リモートホストアドレス（Remote Host Address）]** の IP アドレスおよびオプションの [セカンダリアドレス（Secondary Address）]（冗長データインターフェイスを使用する場合）または [編集（Edit）]（✎）をクリックしてホスト名を編集します。

図 *12*：管理アドレスの編集



b) [管理（Management）] ダイアログボックスの **[リモートホストアドレス（Remote Host Address）]** フィールドおよびオプションの [セカンダリアドレス（Secondary Address）] フィールドで名前または IP アドレスを変更し、[保存（Save）] をクリックします。

図 *13*：管理 *IP* アドレス



ステップ 3 Firewall Management Center の IP アドレスを変更してください。

注意
Firewall Management Center インターフェイスを変更する場合は十分にご注意ください。設定エラーのために再接続できない場合は、Firewall Management Center コンソールポートにアクセスして、Linux シェルでネットワーク設定を再設定する必要があります。この操作では、Cisco TAC に連絡する必要があります。

a) [システム（System）]（⚙）>**[設定（Configuration）]**>**[管理インターフェイス（Management Interfaces）]**を選択します。
b) [インターフェイス（Interfaces）] エリアで、設定するインターフェイスの横にある [編集（Edit）] をクリックします。
c) IP アドレスを変更し、[保存（Save）] をクリックします。

ステップ 4 デバイスのマネージャ IP アドレスを変更します。

高可用性ペアまたはクラスタの場合は、すべてのユニットでこれらの CLI 手順を実行します。

a) Firewall Threat Defense CLI で、Firewall Management Center 識別子を表示します。

show managers

例：

```
> show managers
Type                       : Manager
Host                       : 10.10.1.4
Display name               : 10.10.1.4
Identifier                 : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration               : Completed
Management type            : Configuration
```

b) Firewall Management Center IP アドレスまたはホスト名を編集します。

configure manager edit *identifier* {**hostname** {*ip_address* | *hostname*} | **displayname** *display_name*}

Firewall Management Center が **DONTRESOLVE** と NAT ID によって最初に識別された場合、このコマンドを使用して値をホスト名または IP アドレスに変更できます。IP アドレスまたはホスト名を **DONTRESOLVE** に変更することはできません。

例：

```
> configure manager edit f7ffad78-bf16-11ec-a737-baa2f76ef602 hostname 10.10.5.1
```

ステップ 5 コンソールポートでマネージャ アクセス インターフェイスの IP アドレスを変更します。

高可用性ペアまたはクラスタの場合は、すべてのユニットでこれらの CLI 手順を実行します。

専用管理インターフェイスを使用している場合：

configure network ipv4

configure network ipv6

専用管理インターフェイスを使用している場合：

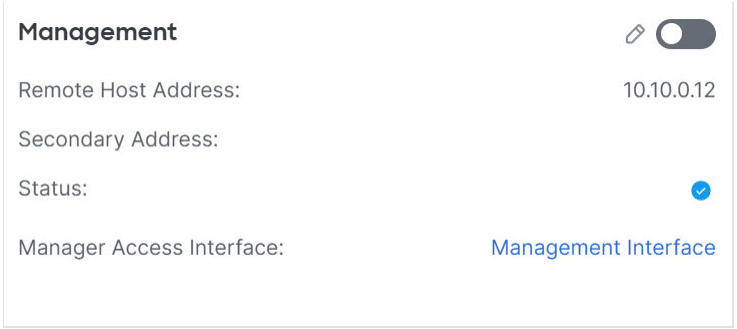
configure network management-data-interface disable

configure network management-data-interface

ステップ 6 スライダをクリックして管理を再度有効（  ）にします。

高可用性ペアまたはクラスタの場合は、すべてのユニットでこれらの CLI 手順を実行します。

図 *14 :* 管理接続の有効化



ステップ 7 （マネージャアクセスにデータインターフェイスを使用している場合）Firewall Management Center でデータインターフェイス設定を更新します。

高可用性ペアの場合は、両方のユニットでこの手順を実行します。

a) **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [管理（Management）] > [マネージャアクセス - 構成詳細（Manager Access - Configuration Details）]** を選択し、[更新（Refresh）] をクリックします。

b) **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）]** を選択し、新しいアドレスと一致するように IP アドレスを設定します。

c) [マネージャアクセス - 構成詳細（Manager Access - Configuration Details）] [FMCアクセス - 構成詳細（FMC Access - Configuration Details] ダイアログボックスに戻り、[確認（Acknowledge）] をクリックして展開ブロックを削除します。

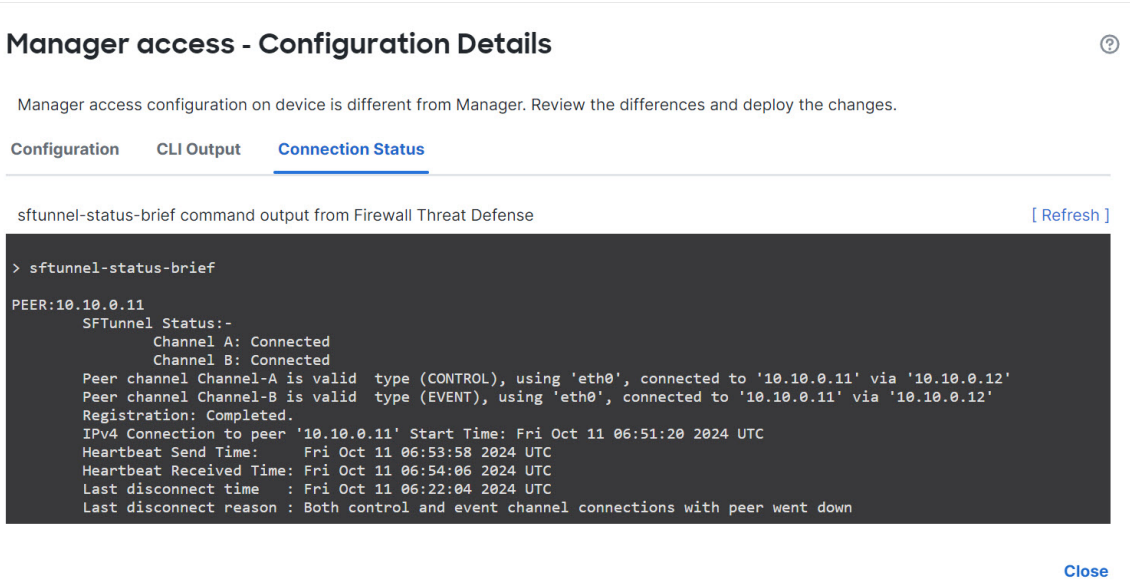
ステップ 8 管理接続が再確立されたことを確認します。

Firewall Management Center で、**[Devices] > [Device Management] > [Device] > [Management] > [Manager Access - Configuration Details] > [Connection Status]** ページで管理接続ステータスを確認します。

管理接続のステータスを表示するには、Firewall Threat Defense CLI で、**sftunnel-status-brief** コマンドを入力します。

次のステータスは、データインターフェイスの接続が成功したことを示し、内部の「tap_nlp」インターフェイスを示しています。

図 *15* : 接続ステータス



ステップ 9 （高可用性 Firewall Management Center ペアの場合）セカンダリ Firewall Management Center で設定変更を繰り返します。

a) セカンダリ Firewall Management Center IP アドレスを変更します。
b) 両方のユニットで新しいピアアドレスを指定します。
c) セカンダリユニットをアクティブユニットにします。
d) デバイスの管理接続を無効にします。
e) Firewall Management Center でデバイスの IP アドレスを変更します。
f) 管理接続を再度有効にします。

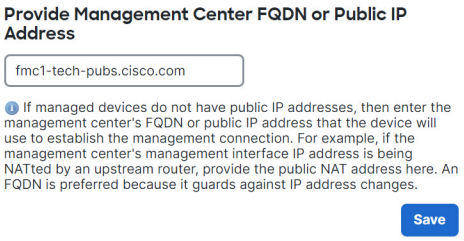
マネージャのリモートアクセス

管理対象デバイスにパブリック IP アドレスまたは FQDN がない場合、またはゼロタッチプロビジョニングの管理インターフェイスを使用する場合は、デバイスが管理接続を開始できるように Firewall Management Center のパブリック IP アドレス/FQDN を設定します。

たとえば、Firewall Management Center の管理インターフェイスの IP アドレスが上流のルータによって NAT されている場合は、ここにパブリック NAT アドレスを入力します。IP アドレスの変更を防ぐため、FQDN が優先されます。

シリアル番号（ゼロタッチプロビジョニング）方式を使用してデバイスを登録する場合、このフィールドはマネージャの IP アドレス/ホスト名の初期設定に自動的に使用されます。手動登録キー方式を使用する場合は、デバイスの初期構成を実行するときにこの画面の値を参照すると、パブリック Firewall Management Center IP アドレス/ホスト名を特定できます。

図 *16 :* マネージャのリモートアクセス



ネットワーク分析ポリシーの設定

ユーザーがネットワーク分析ポリシーを変更した場合、ポリシー関連の変更をコメント機能を使用してトラッキングするようにシステムを設定できます。ポリシー変更のコメントが有効にされていると、管理者はコメントにアクセスして、導入で重要なポリシーが変更された理由を素早く評価できます。

ポリシーの変更に関するコメントを有効にした場合、コメントをオプションまたは必須に設定できます。システムは、ポリシーに対する新しい変更が保存されるたびに、ユーザーにコメントを入力するようプロンプトを出します。

オプションで、ネットワーク分析ポリシーに対する変更を監査ログに書き込むこともできます。

プロセス

Firewall Management Center のプロセスのシャットダウンおよび再起動を制御するには、Web インターフェイスを使用します。次の操作を実行できます。

- シャットダウン：アプライアンスのグレースフル シャットダウンを開始します。

⚠

注意 電源ボタンを使用して Cisco Secure Firewall アプライアンスを停止しないでください。データが失われる可能性があります。Web インターフェイス（または CLI）を使用すると、設定データを失うことなく、安全にシステムの電源を切って再起動する準備が整います。

- リブート：シャットダウンしてグレースフルに再起動します。
- コンソールの再起動：通信、データベース、HTTP サーバーのプロセスを再起動します。これは通常、トラブルシューティングの際に使用されます。

ヒント　仮想デバイスの場合は、ご使用の仮想プラットフォームのマニュアルを参照してください。特に VMware の場合、カスタム電源オプションは VMware ツールの一部です。

Firewall Management Center のシャットダウンまたは再起動

手順

ステップ 1　[システム（System）]（⚙）>**[構成（Configuration）]**を選択します。

ステップ 2　[プロセス（Process）] を選択します。

ステップ 3　次のいずれかを実行します。

シャットダウン	[管理センターのシャットダウン（Shutdown Management Center）] の横にある [コマンドの実行（Run Command）] をクリックします。
再起動	[管理センターの再起動（Reboot Management Center）] の横にある [コマンドの実行（Run Command）] をクリックします。 （注） 再起動するとログアウトします。システムはデータベース チェックを実行しますが、これは完了するのに 1 時間かかります。
コンソールの再起動	[管理センターコンソールの再起動（Restart Management Center Console）] の横にある [コマンドの実行（Run Command）] をクリックします。 （注） 再起動すると、ネットワーク マップ内に削除されたホストが再表示されることがあります。

REST API 設定

Management Center の REST API は、サードパーティ アプリケーションで REST クライアントおよび標準 HTTP メソッドを使用してデバイス設定を表示および管理するための軽量のインターフェイスを提供します。Management Center の REST API の詳細については、Cisco Secure Firewall Management Center REST API クイックスタートガイド を参照してください。

（注）　HTTPS 証明書は、Management Center の REST API ではサポートされていません。

デフォルトでは、Firewall Management Center はアプリケーションからの REST API を使用した要求を許可します。このアクセスをブロックするように Firewall Management Center を設定できます。

REST API アクセスの有効化

（注） Firewall Management Center 高可用性を使用する展開では、この機能は、アクティブな Firewall Management Center でのみ使用できます。

手順

ステップ 1 [システム（System）]（⚙）>**[構成（Configuration）]** を選択します。

ステップ 2 [REST API 設定（REST API Preferences）] をクリックします。

ステップ 3 Firewall Management Center への REST API アクセスを有効または無効にするには、[REST API の有効化（Enable REST API）] チェックボックスをオンまたはオフにします。

ステップ 4 **[Save]** をクリックします。

ステップ 5 `https://<management_center_IP_or_name>:<https_port>/api/api-explorer` で REST API エクスプローラにアクセスします。

リモート コンソールのアクセス管理

サポート対象システム上でリモート アクセスを行うため、VGA ポート（デフォルト）または物理アプライアンス上のシリアル ポートを介して Linux システムのコンソールを使用できます。[コンソール設定（Console Configuration）] ページを使用して、組織の Cisco Secure Firewall 展開環境の物理レイアウトに最も適したオプションを選択します。

サポートされている物理ハードウェアベースのシステムでは、Serial Over LAN（SOL）接続で Lights-Out 管理（LOM）を使用すると、システムの管理インターフェイスにログインすることなく、リモートでシステムをモニターまたは管理できます。アウト オブ バンド管理接続のコマンドラインインターフェイスを使用すると、シャーシのシリアル番号の表示や状態（ファン速度や温度など）のモニタなどの、限定タスクを実行できます。LOM をサポートするケーブル接続は、Firewall Management Center モデルによって異なります。

- Firewall Management Center モデル MC1600、MC2600、および MC4600 では、CIMC ポートとの接続を使用して LOM をサポートします。詳細は、『*Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide*』を参照してください。
- 他のすべての Firewall Management Center ハードウェアモデルでは、LOM をサポートするためにデフォルト（eth0）管理ポートとの接続を使用します。ご使用のハードウェアモデ

ルの『*Navigating the Cisco Secure Firewall Threat Defense Documentation Guide*』『』を参照してください。

LOM は、システムとシステムを管理するユーザーの両方で有効にする必要があります。システムとユーザーを有効にした後、サードパーティ製の Intelligent Platform Management Interface（IPMI）ユーティリティを使用し、システムにアクセスして管理します。

システム上のリモート コンソール設定の構成

この手順を実行するには、管理者ユーザーである必要があります。

始める前に

- デバイスの管理インターフェイスに接続されたサードパーティ スイッチング装置で、スパニング ツリー プロトコル（STP）を無効にします。
- Lights-Out 管理を有効にする予定がある場合、インテリジェント プラットフォーム管理インターフェイス（IPMI）ユーティリティのインストールと使用については、アプライアンスのスタートアップガイドを参照してください。

手順

ステップ 1 [システム（System）]（⚙）>**[構成（Configuration）]**を選択します。

ステップ 2 [コンソール構成（Console Configuration）] をクリックします。

ステップ 3 リモート コンソール アクセスのオプションを選択します。

- アプライアンスの VGA ポートを使用するには、[VGA] を選択します。
- アプライアンスのシリアルポートを使用する場合には、[物理シリアルポート（Physical Serial Port）] を選択します。
- Firewall Management Center で SOL 接続を使用するには、[Lights-Out管理（Lights-Out Management）] を選択します。（お使いの Firewall Management Center モデルに応じて、デフォルトの管理ポートまたはCIMC ポートを使用する場合があります。詳細については、モデルのスタートアップガイドを参照してください）。

ステップ 4 SOL を介して LOM を構成するには：

- システムのアドレスの [構成（Configuration）]（[DHCP] または [Manual（手動）]）を選択します。
- 手動構成を選択した場合は、必要な IPv4 設定を入力します。
  - LOM に使用する IP アドレスを入力します。

（注）

LOM IP アドレスは、Firewall Management Center管理インターフェイスの IP アドレスとは異なり、かつ同じサブネット内にある必要があります。

- システムのネットマスクを入力します。
- システムのデフォルト ゲートウェイを入力します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 「これらの変更を有効にするためには、システムを再起動する必要があります（You will have to reboot your system for these changes to take effect）」という警告が表示されます。[OK] をクリックしてすぐに再起動するか、[キャンセル（Cancel）] をクリックして後で再起動します。

次のタスク

- シリアルアクセスを設定した場合は、背面パネルのシリアルポートが、ローカルコンピュータ、ターミナルサーバー、またはお使いの Firewall Management Center モデルのスタートアップガイドで説明されている、イーサネット経由のリモートシリアルアクセスをサポートできるその他のデバイスに接続されていることを確認します。
- Lights-Out Management を設定した場合は、Lights-Out Management ユーザーを有効にします。Lights-Out 管理のユーザー アクセス設定 （72 ページ）を参照してください。

Lights-Out 管理のユーザー アクセス設定

Lights-Out 管理機能を使用するユーザーに対して、この機能の権限を明示的に付与する必要があります。LOM ユーザーには、次のような制約もあります。

- ユーザーに Administrator ロールを割り当てる必要があります。
- ユーザー名に使用できるのは英数字 16 文字までです。LOM ユーザーに対し、ハイフンやそれより長いユーザー名はサポートされていません。
- ユーザーの LOM パスワードは、そのユーザーのシステム パスワードと同じです。パスワードは、ユーザパスワードで説明されている要件に準拠している必要があります。辞書に載っていない複雑な最大長のパスワードをアプライアンスに対して使用し、それを 3 か月ごとに変更することを推奨します。
- 物理 Firewall Management Center には、最大 13 人の LOM ユーザーを設定できます。

あるユーザーのログイン中に LOM でそのユーザーを非アクティブ化してから再アクティブ化した場合、そのユーザーは `ipmitool` コマンドへのアクセスを回復するために Web インターフェイスへのログインし直しが必要になることがあります。

（注） 高可用性同期は LOM ユーザーには適用されないため、高可用性 Firewall Management Center ではそれらのユーザーが複製されません。アクティブな Firewall Management Center で LOM を有効にした別の管理者ユーザーを作成する必要があります。

高可用性構成で、ローカルユーザーを作成するか、LOM 権限が有効になっているローカルユーザーのパスワードをリセットすると、その変更が、UCS ベースのアクティブな Firewall Management Center から、アクティブおよびスタンバイの両方の Firewall Management Center とアクティブな Firewall Management Center CIMC に同期されます。新しいパスワードは、CIMC ログイン用にスタンバイ Firewall Management Center と同期されません。スタンバイ Firewall Management Center も更新されるようにするには、スタンバイ Firewall Management Center のローカルユーザーの CIMC ログインパスワードをリセットします。

Lights-Out 管理ユーザー アクセスの有効化

この手順を実行するには、管理者ユーザーである必要があります。

このタスクを使用して、既存のユーザーに LOM アクセスを許可します。新しいユーザーに LOM アクセスを許可するには、内部ユーザーの追加または編集を参照してください。

手順

ステップ 1 [システム（System）]（⚙）>**[ユーザー（Users）]**>**[ユーザー（Users）]**を選択します。

ステップ 2 既存のユーザーに LOM ユーザーアクセスを許可するには、リスト内のユーザー名の横にある [編集（Edit）]（✎）をクリックします。

ステップ 3 [ユーザーの設定（User Configuration）] で、Administrator ロールを有効にします。

ステップ 4 [Lights-Out 管理アクセスの許可（Allow Lights-Out Management Access）] チェックボックスをオンにします。

ステップ 5 [保存（Save）] をクリックします。

Serial over LAN 接続の設定

アプライアンスへの Serial over LAN 接続を作成するには、コンピュータ上でサードパーティ製の IPMI ユーティリティを使用します。Linux 系環境または Mac 環境を使用するコンピュータでは IPMItool を使用します。Windows 環境では、使用している Windows バージョンによって IPMIutil または IPMItool を使用できます。

（注） シスコでは、IPMItool バージョン 1.8.12 以降の使用を推奨しています。

Linux

多くのディストリビューションで IPMItool が標準となっており、使用可能です。

Mac

Mac では、IPMItool をインストールする必要があります。最初に、Mac に Apple の XCode Apple Developer Tools がインストールされていることを確認します。これにより、コマンドライン開発用のオプション コンポーネント（新しいバージョンでは UNIX Development and System Tools、古いバージョンでは Command Line Support）がインストールされていることを確認できます。次に、MacPorts と IPMItool をインストールします。詳細については、好みの検索エンジンを使用するか、次のサイトを参照してください。

```
https://developer.apple.com/technologies/tools/
http://www.macports.org/
http://github.com/ipmitool/ipmitool/
```

Windows

Windows Subsystem for Linux（WSL）が有効になっている Windows バージョン 10 以降、および一部の古いバージョンの Windows Server では、IPMItool を使用できます。それ以外の場合は、Windows システムで IPMIutil をコンパイルする必要があります。IPMIutil 自体を使用してコンパイルできます。詳細については、好みの検索エンジンを使用するか、次のサイトを参照してください。

```
http://ipmiutil.sourceforge.net/man.html#ipmiutil
```

IPMI ユーティリティのコマンドについて

IPMI ユーティリティで使用するコマンドは、Mac での IPMItool に関する次の例に示したセグメントで構成されます。

```
ipmitool -I lanplus -H IP_address -U user_name command
```

引数の説明

- `ipmitool` はユーティリティを起動します。
- `-I lanplus` は、セッションに暗号化された IPMI v2.0 RMCP+ LAN インターフェイスを使用することを指定します。
- `-H IP_address` はアクセスするアプライアンスの Lights-Out 管理用に設定された IP アドレスを示します。
- `-U user_name` は権限を持つユーザーの名前です。
- `command` は使用するコマンドの名前です。

（注） シスコでは、IPMItool バージョン 1.8.12 以降の使用を推奨しています。

Windows での IPMIutil の同じコマンドは、次のようになります。

```
ipmiutil command -V 4 -J 3 -N IP_address -Uuser_name
```

このコマンドは、アプライアンスのコマンドラインにユーザーを接続します。これによって、ユーザーは物理的にそのアプライアンスの近くにいるときと同じようにログインできます。場合によっては、パスワードの入力を求められます。

IPMItool を使用した Serial Over LAN の設定

この手順を実行するには、LOM アクセス権限のある管理者ユーザーである必要があります。

手順

IPMItool を使用して、次のコマンドと、プロンプトが表示されたらパスワードを入力します:

```
ipmitool -I lanplus -H IP_address -U user_name sol activate
```

IPMIutil を使用した Serial Over LAN の設定

この手順を実行するには、LOM アクセス権限のある管理者ユーザーである必要があります。

手順

IPMIutil を使用して、次のコマンドと、プロンプトが表示されたらパスワードを入力します。

```
ipmiutil -J 3 -N IP_address -U username sol -a
```

Lights-Out 管理の概要

Lights-Out 管理（LOM）では、システムにログインすることなく、デフォルトの管理インターフェイス（eth0）から SOL 接続を介して一連の限定操作を実行できます。SOL 接続を作成するコマンドに続いて、次のいずれかの LOM コマンドを使用します。コマンドが完了すると、接続は終了します。

注意 まれに、コンピュータがシステムの管理インターフェイスとは異なるサブネットにあり、そのシステムに DHCP が構成されている場合は、LOM 機能にアクセスしようとすると失敗することがあります。この場合は、システムの LOM を無効にして再び有効にするか、または同じサブネット上のコンピュータをシステムとして使用して、その管理インターフェイスを ping することができます。その後、LOM を使用できるようになるはずです。

注意 シスコでは、Intelligent Platform Management Interface（IPMI）標準（CVE-2013-4786）に内在する脆弱性を認識しています。システムの Lights-Out 管理（LOM）を有効にすると、この脆弱性にさらされます。この脆弱性を軽減するために、信頼済みユーザーだけがアクセス可能なセキュアな管理ネットワークにシステムを展開し、辞書に載っていない複雑な最大長のパスワードをシステムに対して使用し、それを 3 か月ごとに変更してください。この脆弱性のリスクを回避するには、LOM を有効にしないでください。

システムへのアクセス試行がすべて失敗した場合は、LOM を使用してリモートでシステムを再起動できます。SOL 接続がアクティブなときにシステムが再起動すると、LOM セッションが切断されるか、またはタイムアウトする可能性があります。

注意 システムが別の再起動の試行に応答している間は、システムを再起動**しないでください**。リモートでシステムを再起動すると、通常の方法でシステムがリブートしないため、データが失われる可能性があります。

表 *4 : Lights-Out* 管理のコマンド

IPMItool	IPMIutil	説明
（非該当）	`-V 4`	IPMI セッションの管理者権限を有効にします
`-I lanplus`	`-J 3`	IPMI セッションの暗号化を有効にします
`-H` *`hostname/IP address`*	`-N` *`nodename/IP address`*	次の LOM IP アドレスまたはホスト名を示しま Firewall Management Center
`-U`	`-U`	認可された LOM アカウントのユーザー名を指 ます
`sol activate`	`sol -a`	SOL セッションを開始します
`sol deactivate`	`sol -d`	SOL セッションを終了します
`chassis power cycle`	`power -c`	アプライアンスを再起動します
`chassis power on`	`power -u`	アプライアンスの電源を投入します

IPMItool	IPMIutil	説明
chassis power off	power -d	アプライアンスの電源をオフにします
sdr	sensor	アプライアンスの情報（ファン速度や温度を表示します

たとえば、アプライアンスの情報のリストを表示する IPMItool のコマンドは、次のとおりです。

```
ipmitool -I lanplus -H IP_address -U user_name sdr
```

（注） シスコでは、IPMItool バージョン 1.8.12 以降の使用を推奨しています。

IPMIutil ユーティリティの同等のコマンドは次のとおりです。

```
ipmiutil sensor -V 4 -J 3 -N IP_address -U user_name
```

IPMItool を使用した Lights-Out 管理の設定

この手順を実行するには、LOM アクセス権限のある管理者ユーザーである必要があります。

手順

プロンプトが表示されたら、IPMItool の次のコマンドとパスワードを入力します。

```
ipmitool -I lanplus -H IP_address -U user_name command
```

IPMIutil を使用した Lights-Out 管理の設定

この手順を実行するには、LOM アクセス権限のある管理者ユーザーである必要があります。

手順

プロンプトが表示されたら、IPMIutil の次のコマンドとパスワードを入力します。

```
ipmiutil -J 3 -N IP_address -U username command
```

リモート ストレージ デバイス

Firewall Management Center のバックアップおよびレポートをローカルに保存したり、次のいずれかのシステムをマウントすることができます。

- ネットワーク ファイル システム（NFS）
- サーバ メッセージ ブロック（SMB）/Common Internet File System（CIFS）
- Secure Shell Filesystem（SSHFS）

1 つのリモート システムにバックアップを送信し、別のリモート システムにレポートを送信することはできませんが、どちらかをリモート システムに送信し、もう一方を Firewall Management Center に格納することは可能です。

ヒント リモート ストレージを構成して選択した後は、接続データベースの制限を増やさなかった場合にのみ、ローカル ストレージに戻すことができます。「データベース （30 ページ）」を参照してください。

ローカル ストレージの設定

手順

ステップ 1 [システム（System）]（⚙）>**[構成（Configuration）]**を選択します。
ステップ 2 [リモート ストレージ デバイス（Remote Storage Device）] を選択します。
ステップ 3 [ストレージ タイプ（Storage Type）] ドロップダウン リストから [ローカル（リモート ストレージなし）（Local (No Remote Storage)）] を選択します。
ステップ 4 [保存（Save）] をクリックします。

リモートストレージの NFS の設定

Firewall Management Center は、 NFS マウントでバックアップとレポートを保存できます。

手順

ステップ 1 [システム（System）]（⚙）>**[構成（Configuration）]**を選択します。
ステップ 2 [リモート ストレージ デバイス（Remote Storage Device）] をクリックします。

ステップ 3 [ストレージ タイプ（Storage Type）] ドロップダウン リストから [NFS] を選択します。

ステップ 4 接続情報を追加します。

- [Host] フィールドに、ストレージ システムの IPv4 アドレスまたはホスト名を入力します。
- [ディレクトリ（Directory）] フィールドに、ストレージ領域へのパスを入力します。

ステップ 5 必要に応じて、**[詳細オプションの使用（Use Advanced Options）]** チェックボックスをオンにして、**[コマンド ライン オプション（Command Line Options）]** に必要なマウント オプションを入力します。

次の形式を使用して、NFS ストレージのバージョン番号を指定できます。

vers=*version*

たとえば、NFSv4 を選択するには、次のように入力します。

vers=4.0

ステップ 6 [システムの使用方法（System Usage）] で、次の手順を実行します。

- 指定したホストにバックアップを格納するには、[バックアップに使用（Use for Backups）] を選択します。
- 指定したホストにレポートを格納するには、[レポートに使用（Use for Reports）] を選択します。
- リモート ストレージへのバックアップに関する [ディスク容量のしきい値（Disk Space Threshold）] を入力します。デフォルトは 90% です。

ステップ 7 **[テスト（Test）]** をクリックして接続をテストします。

ステップ 8 [保存（Save）] をクリックします。

トラブルシューティング

ファイアウォールデバイスとの NFS 接続にランダムな遅延がある場合は、次のアクティビティを実行してから、トラブルシューティングについて Cisco TAC にお問い合わせください。

- 問題の発生前または発生後に、デバイスからトラブルシューティング ファイルを収集します。トラブルシューティング ファイルは、Web インターフェイスから、または CLI コマンドを使用して生成できます。トラブルシューティング ファイルの生成方法については、『Troubleshoot Firepower File Generation Procedures』を参照してください。
- 着信トラフィックと発信トラフィックの PCAP レコードを収集します。手順については、パケット キャプチャの概要を参照してください。
- デバイスで次のコマンドを使用して（CLISH モード）、NFS アプリケーションの障害発生中にシステム サポート トレース データを収集します。

```
> system support trace
```

- **show snort counters** コマンドを使用して、障害発生中に Snort カウンタを 2 回収集し、Snort プリプロセッサ接続の統計を表示します。このコマンドについては、「show snort counters」を参照してください。

リモート ストレージ用の SMB の設定

Firewall Management Center は、 SMB マウントでバックアップとレポートを保存できます。

始める前に

外部リモートストレージシステムが機能していて、Firewall Management Center からアクセスできることを確認します。

- システムに認識されるのは、ファイルのフルパスではなく、最上位の SMB 共有です。使用する正確なディレクトリを共有するには、Windows を使用する必要があります。
- Firewall Management Center から SMB 共有にアクセスするために使用する Windows ユーザーが、共有場所の読み取り/変更のアクセス権を持っていることを確認してください。
- セキュリティを確保するには、SMB 2.0 以降をインストールする必要があります。

手順

ステップ 1 [システム（System）]（⚙）>**[構成（Configuration）]**を選択します。

ステップ 2 [リモート ストレージ デバイス（Remote Storage Device）] をクリックします。

ステップ 3 [ストレージ タイプ（Storage Type）] ドロップダウン リストから [SMB] を選択します。

ステップ 4 接続情報を追加します。

- [Host] フィールドに、ストレージ システムの IPv4 アドレスまたはホスト名を入力します。
- [Share] フィールドに、ストレージ領域の共有を入力します。
- 必要に応じて、[Domain] フィールドにリモート ストレージ システムのドメイン名を入力します。
- [ユーザー名（Username）] フィールドにストレージ システムのユーザー名を入力し、[パスワード（Password）] フィールドにそのユーザーのパスワードを入力します。

ステップ 5 必要に応じて、**[詳細オプションの使用（Use Advanced Options）]** チェックボックスをオンにして、**[コマンド ライン オプション（Command Line Options）]** に必要なマウント オプションを入力します。

次の形式を使用して、SMB ストレージのバージョン番号を指定できます。

vers=*version*

ファイルサーバーで SMB 暗号化が有効になっている場合、SMB バージョン 3.0 クライアントのみがファイルサーバーにアクセスできます。この場合は、次のように入力します：

vers=3.0

ステップ 6 [システムの使用方法（System Usage）] で、次の手順を実行します。

- 指定したホストにバックアップを格納するには、[バックアップに使用（Use for Backups）] を選択します。
- 指定したホストにレポートを格納するには、[レポートに使用（Use for Reports）] を選択します。

ステップ 7 設定をテストするには、[テスト（Test）] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

リモート ストレージ用の SSH の設定

Firewall Management Center は、SSHFS マウントでバックアップとレポートを保存できます。

手順

ステップ 1 [システム（System）]（⚙）>**[構成（Configuration）]**を選択します。

ステップ 2 [リモート ストレージ デバイス（Remote Storage Device）] をクリックします。

ステップ 3 [ストレージ タイプ（Storage Type）] ドロップダウン リストから [SSH] を選択します。

ステップ 4 接続情報を追加します。

- [ホスト（Host）] フィールドに、ストレージ システムの IP アドレスまたはホスト名を入力します。
- [ディレクトリ（Directory）] フィールドに、ストレージ領域へのパスを入力します。
- [ユーザー名（Username）] フィールドにストレージ システムのユーザー名を入力し、[パスワード（Password）] フィールドにそのユーザーのパスワードを入力します。接続ユーザー名の一部としてネットワーク ドメインを指定するには、ユーザー名の前にドメインを入力し、スラッシュ（/）で区切ります。
- SSH キーを使用するには、[SSH 公開キー（SSH Public Key）] フィールドの内容をコピーして authorized_keys ファイルに貼り付けます。

ステップ 5 必要に応じて、**[詳細オプションの使用（Use Advanced Options）]** チェックボックスをオンにして、**[コマンド ライン オプション（Command Line Options）]** に必要なマウント オプションを入力します。

ステップ 6 [システムの使用方法（System Usage）] で、次の手順を実行します。

- 指定したホストにバックアップを格納するには、[バックアップに使用（Use for Backups）] を選択します。
- 指定したホストにレポートを格納するには、[レポートに使用（Use for Reports）] を選択します。

ステップ 7 **[テスト（Test）]** をクリックして接続をテストします。

ステップ 8 [保存（Save）] をクリックします。

SNMP

Simple Network Management Protocol （SNMP）のポーリングを有効にできます。SNMP 機能は、SNMP プロトコルのバージョン 1、2、3 をサポートします。この機能を使用すると、標準 Management Information Base（MIB）にアクセスできます。MIB には、連絡先、管理、場所、サービス情報、IP アドレッシングやルーティングの情報、トランスミッション プロトコルの使用状況の統計などのシステムの詳細が含まれます。

（注） SNMP プロトコルの SNMP バージョンを選択する場合、SNMPv2 では読み取り専用コミュニティのみがサポートされ、SNMPv3 では読取り専用ユーザーのみがサポートされることに注意してください。SNMPv3 は、AES128 での暗号化をサポートします。

SNMP ポーリングを有効にすると、システムで SNMP トラップを送信できなくなり、MIB の情報はネットワーク管理システムによるポーリングでのみ使用可能になります。

SNMP ポーリングの設定

始める前に

使用するコンピュータごとに SNMP アクセスを追加し、システムをポーリングします。アクセス リストの設定 （13 ページ）を参照してください。

（注） SNMP MIB には展開の攻撃に使用される可能性がある情報が含まれています。SNMP アクセスのアクセス リストを MIB のポーリングに使用される特定のホストに制限することを推奨します。SNMPv3 を使用し、ネットワーク管理アクセスには強力なパスワードを使用することも推奨します。

手順

ステップ 1 [システム（System）]（⚙）> **[構成（Configuration）]** を選択します。

ステップ 2 [SNMP] をクリックします。

ステップ 3 [SNMPバージョン（SNMP Version）] ドロップダウン リストから、使用する SNMP バージョンを選択します。

- [Version 1] または [Version 2]：[Community String] フィールドに読み取り専用の SNMP コミュニティ名を入力してから、手順の最後までスキップします。

  （注）
  SNMP コミュニティストリング名には、特殊文字（<>/%#&?',etc.）を使用できません。

- [バージョン3（Version 3）]：[ユーザーを追加（Add User）] をクリックすると、ユーザー定義ページが表示されます。SNMPv3 は、読み取り専用ユーザーと AES128 による暗号化のみをサポートしています。

ステップ 4 ユーザー名を入力します。

ステップ 5 [認証プロトコル（Authentication Protocol）] ドロップダウン リストから、認証に使用するプロトコルを選択します。

ステップ 6 [認証パスワード（Authentication Password）] フィールドに SNMP サーバーの認証に必要なパスワードを入力します。

ステップ 7 [パスワードの確認（Verify Password）] フィールドに、認証パスワードを再度入力します。

ステップ 8 使用するプライバシー プロトコルを [プライバシー プロトコル（Privacy Protocol）] リストから選択するか、プライバシー プロトコルを使用しない場合は [なし（None）] を選択します。

ステップ 9 [プライバシー パスワード（Privacy Password）] フィールドに SNMP サーバーで必要な SNMP プライバシー キーを入力します。

ステップ 10 [パスワードの確認（Verify Password）] フィールドに、プライバシー パスワードを再度入力します。

ステップ 11 [追加（Add）] をクリックします。

ステップ 12 [保存（Save）] をクリックします。

セッション タイムアウト

無人ログインセッションは、セキュリティ上のリスクを生じさせる場合があります。ユーザーのログインセッションが非アクティブになったためにタイムアウトするまでのアイドル時間を設定できます。

システムを長期間にわたってパッシブかつセキュアにモニターする予定のシナリオでは、特定の Web インターフェイスのユーザーがタイムアウトしないように設定できることに注意してください。メニューオプションへの完全なアクセス権がある管理者ロールのユーザーは、侵害が生じる場合、余分のリスクを生じさせますが、セッションタイムアウトから除外することはできません。

セッション タイムアウトの設定

手順

ステップ 1 [システム（System）]（⚙）>**[構成（Configuration）]**を選択します。

ステップ 2 [CLIタイムアウト（CLI Timeout）] をクリックします。

ステップ 3 セッション タイムアウトの設定

- Web インターフェイス（Firewall Management Center のみ）：[ブラウザセッションタイムアウト（分）（Browser Session Timeout (Minutes)）] を設定します。デフォルト値は 60 で、最大値は 1440（24 時間）です。

  このセッションタイムアウトからユーザーを除外する場合は、内部ユーザーの追加または編集を参照してください。

- CLI：[CLIタイムアウト（分）（CLI Timeout (Minutes)）] フィールドを設定します。デフォルト値は 0 で、最大値は 1440（24 時間）です。

ステップ 4 [保存（Save）] をクリックします。

時刻（Time）

[ユーザー設定（User Preferences）] の [タイムゾーン（Time Zone）] ページで設定したタイムゾーン（デフォルトでは America/New York）を使用すると、ほとんどのページでローカル時刻で時刻設定が表示されますが、アプライアンスには UTC 時間を使用して格納されます。

制約事項 タイムゾーン機能（[ユーザー設定（User Preferences）]）は、デフォルトのシステム クロックが UTC 時間に設定されていることを前提としています。システム時刻を変更しようとしないでください。システム時刻の UTC からの変更はサポートされていません。また、システム時刻を変更した場合はデバイスを再イメージ化してサポートされていない状態から回復させる必要があります。

手順

ステップ 1 [システム（System）]（⚙）>**[構成（Configuration）]**を選択します。

ステップ 2 [時間（Time）] をクリックします。

現在の時刻は、[ユーザー設定（User Preferences）] でアカウントに指定されたタイムゾーンを使用して表示されます。

アプライアンスで NTP サーバを使用する場合、テーブル エントリについては、NTP サーバーのステータス （85 ページ）を参照してください。

NTP サーバーのステータス

NTP サーバーから時刻を同期する場合は、[時間（Time）] ページ（[システム（System）] > [設定（Configuration）] を選択）で接続ステータスを確認できます。

表 *5 : NTP* ステータス

列	説明
NTP サーバー	設定済みの NTP サーバーの IP アドレスまたは名前。
ステータス	NTP サーバの時間同期のステータス。 • [使用中（Being Used）] は、アプライアンスが NTP サーバと同期していることを示します。 • [使用可能（Available）] は、NTP サーバーが使用可能であるものの、時間がまだ同期していないことを示します。 • [使用不能（Not Available）] は、NTP サーバーが構成に含まれているものの、NTP デーモンがその NTP サーバーを使用できないことを示します。 • [保留（Pending）] は、NTP サーバーが新しいか、または NTP デーモンが最近再起動されたことを示します。この値は、時間の経過とともに [使用中（Being Used）]、[使用可能（Available）]、または [使用不能（Not Available）] に変わるはずです。 • [不明（Unknown）] は、NTP サーバーのステータスが不明であることを示します。
認証	Firewall Management Center と NTP サーバー間の通信の認証ステータスは次のとおりです。 • [なし（none）] は、認証が設定されていないことを示します。 • [不良（bad）] は、認証が設定されているが失敗していることを示します。 • [OK] は認証が成功したことを示します。 認証が設定されている場合、ステータス値の後にキー番号とキータイプ（SHA-1、MD5、または AES-128 CMAC）が表示されます。例：[不良、キー2、MD5（bad, key 2, MD5）]。

列	説明
オフセット	アプライアンスと構成済みの NTP サーバ間の時間の差（ミリ秒）。負の値はアプライアンスの時間が NTP サーバより遅れていることを示し、正の値は進んでいることを示します。
最終更新	NTP サーバと最後に時間を同期してから経過した時間（秒数）。NTP デーモンは、いくつかの条件に基づいて自動的に同期時間を調整します。たとえば、更新時間が大きい（300 秒など）場合、それは時間が比較的安定しており、NTP デーモンが小さい更新増分値を使用する必要がないと判断したことを示します。

時刻の同期

システムを正常に動作させるには、Secure Firewall Management Center（Firewall Management Center）とその管理対象デバイスのシステム時刻を同期させる必要があります。Firewall Management Center 初期設定時に NTP サーバーを指定することを推奨しますが、初期設定の完了後に、このセクションの情報を使用して、時刻同期設定を確立または変更することができます。

Firewall Management Center とすべてのデバイスのシステム時刻を同期させるには、Network Time Protocol（NTP）サーバーを使用します。Firewall Management Center は、MD5、SHA-1、または AES-128 CMAC 対称キー認証を使用して NTP サーバーとのセキュア通信をサポートしています。システムセキュリティについては、この機能を使用することを推奨します。

Firewall Management Center は、認証済みの NTP サーバーのみと接続するように設定することもできます。このオプションを使用すると、混合認証環境で、またはシステムを別の NTP サーバーに移行するときに、セキュリティを向上させることができます。すべての到達可能な NTP サーバーが認証される環境でこの設定を使用することは、冗長になります。

（注） 初期設定時に Firewall Management Center 用の NTP サーバーを指定した場合、その NTP サーバーとの接続は保護されません。MD5、SHA-1、または AES-128 CMAC キーを指定するには、その接続の設定を編集する必要があります。

注意 Firewall Management Center と管理対象デバイスの時刻が同期していないと、意図しない結果になることがあります。

Firewall Management Center と管理対象デバイスの時刻を同期するには、次を参照してください。

- 推奨： Firewall Management Center と NTP サーバー間の時刻の同期 （87 ページ）

このトピックでは、NTP サーバーと同期するように Firewall Management Center を設定する手順と、同じ NTP サーバーと同期するように管理対象デバイスを設定する手順へのリンクを示します。

- 該当しない場合は、次のようになります。 ネットワーク NTP サーバーにアクセスせずに時刻を同期 （89 ページ）

  このトピックでは、Firewall Management Center で時刻を設定する手順、NTP サーバーとして機能するように Firewall Management Center を設定する手順、および Firewall Management Center NTP サーバーと同期するように管理対象デバイスを設定する手順へのリンクを示します。

Firewall Management Center と NTP サーバー間の時刻の同期

システムのすべてのコンポーネント間で時刻を同期することは非常に重要です。

Firewall Management Center とすべての管理対象デバイス間で適切な時刻同期を維持する最適な方法は、ネットワークで NTP サーバーを使用することです。

Firewall Management Center は NTPv4 をサポートします。

この手順を実行するには、管理者権限またはネットワーク管理者権限が必要です。

始める前に

次の点に注意してください。

- Firewall Management Center および管理対象デバイスがネットワーク NTP サーバーにアクセスできない場合は、この手順を使用しないでください。代わりに、ネットワーク NTP サーバーにアクセスせずに時刻を同期 （89 ページ）を参照してください。
- 信頼できない NTP サーバーを指定しないでください。
- NTP サーバーとのセキュアな接続を確立する場合（システムセキュリティに推奨）、NTP サーバーで設定されている SHA-1、MD5、または AES-128 CMAC キーの番号と値を取得します。
- NTP サーバーへの接続では、構成されたプロキシ設定は使用されません。
- Firepower 4100 シリーズ デバイスと Firepower 9300 デバイスでは、この手順を使用してシステム時刻を設定できません。代わりに、この手順を使用して設定するものと同じ NTP サーバーを使用するように、これらのデバイスを設定してください。手順については、ご使用のハードウェアモデル用のマニュアルを参照してください。

注意 Firewall Management Center が再起動され、ここで指定したものとは異なる NTP サーバー レコードを DHCP サーバーが設定した場合、DHCP 提供の NTP サーバーが代わりに使用されます。この状況を回避するには、同じ NTP サーバーを使用するように DHCP サーバーを設定します。

手順

ステップ 1 [システム（System）]（⚙）>**[構成（Configuration）]**を選択します。

ステップ 2 [Time Synchronization] をクリックします。

ステップ 3 [NTPを使用して時間を提供（Serve Time via NTP）] が [有効（Enabled）] の場合、[無効（Disabled）] を選択して、NTP サーバーの Firewall Management Center を無効にします。

ステップ 4 [Set My Clock] オプションの場合、[Via NTP] を選択します。

ステップ 5 [追加（Add）] をクリックします。

ステップ 6 [Add NTP Server] ダイアログボックスで、NTP サーバーのホスト名か IPv4 または IPv6 アドレスを入力します。

ステップ 7 任意Firewall Management Centerと NTP サーバー間の通信を保護するには、次のようにします。

a) [Key Type] ドロップダウンリストから [MD5]、[SHA-1]、または [AES-128 CMAC] を選択します。

b) 指定された NTP サーバーから、対応する MD5、SHA-1、または AES-128 CMAC キー番号とキー値を入力します。

ステップ 8 [Add] をクリックします。

ステップ 9 2つのNTPサーバーのみが設定されている場合、それらのオフセットの差は大きくなります。これにより、Firewall Management Center は、ローカル時刻を使用します。そのため、少なくとも 3 つの NTP サーバーを設定することをお勧めします。

NTP サーバーをさらに追加するには、手順 5 ～ 8 を繰り返します。

ステップ 10 （オプション）Firewall Management Center で正常に認証された NTP サーバーのみを使用するように強制するには、[認証されたNTPサーバーのみを使用する（Use the authenticated NTP server only）] チェックボックスをオンにします。

ステップ 11 [保存（Save）] をクリックします。

次のタスク

管理対象デバイスでは同じ NTP サーバーを使用して同期するように設定します。

- デバイスプラットフォーム設定を指定します：Cisco Secure Firewall Management Center デバイス構成ガイドの「*Configure NTP Time Synchronization for Threat Defense*」。

  Firewall Management Center に NTP サーバーとセキュアな接続を確立するように強制する場合でも（[認証されたNTPサーバーのみを使用する（Use the authenticated NTP server only）]）、そのサーバーへのデバイス接続では認証が使用されないことに注意してください。

- 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。

ネットワーク NTP サーバーにアクセスせずに時刻を同期

デバイスがネットワーク NTP サーバーに直接アクセスできない、または組織内にネットワーク NTP サーバーがない場合は、物理ハードウェア Firewall Management Center を NTP サーバーとして使用できます。

重要

- 他の NTP サーバーがない場合を除き、この手順は使用しないでください。代わりに、Firewall Management Center と NTP サーバー間の時刻の同期 （87 ページ） の手順を使用してください。
- 仮想 Firewall Management Center を NTP サーバーとして使用しません。

Firewall Management Center を NTP サーバーとして設定後、時刻を手動で変更するには、NTP オプションを無効にして時刻を手動で変更してから NTP オプションを再度有効にします。

手順

ステップ 1 Firewall Management Center でシステム時刻を手動で設定するには、次の手順を実行します。

a) [システム（System）]（⚙）>**[構成（Configuration）]**を選択します。
b) [Time Synchronization] をクリックします。
c) [NTP を使用して時間を提供（Serve Time via NTP）] が [有効（Enabled）] の場合、[無効（Disable）] を選択します。
d) [保存（Save）] をクリックします。
e) [マイクロックの設定（Set My Clock）] で、[ローカル設定で手動（Manually in Local Configuration）] を選択します。
f) [保存（Save）] をクリックします。
g) 画面の左側のナビゲーション パネルで [時間（Time）] をクリックします。
h) [時間の設定（Set Time）] ドロップダウン リストを使用して時間を設定します。

（注）
Management Center の時刻を 2 時間以上変更した場合は、誤動作を避けるために、できるだけ早く（たとえばメンテナンスウィンドウで）デバイスを再起動する必要があります。

i) 表示されるタイムゾーンが UTC ではない場合、クリックして、タイムゾーンを [UTC] に設定します。
j) **[Save（保存）]** をクリックします。
k) [Done] をクリックします。
l) [適用（Apply）] をクリックします。

ステップ 2 Firewall Management Center を NTP サーバとして機能するように設定します。

a) 画面の左側のナビゲーション パネルで [時刻同期（Time Synchronization）] をクリックします。

b) [NTPを使用して時間を提供（Serve Time via NTP）] で、[有効（Enabled）] を選択します。
c) [保存（Save）] をクリックします。

ステップ 3 管理対象デバイスでは Firewall Management Center NTP サーバーを使用して同期するように設定します。

a) 管理対象デバイスに割り当てられたプラットフォーム設定ポリシーの [Time Synchronization] 設定で、[Via NTP from Management Center] に同期するようにクロックを設定します。
b) 管理対象デバイスへの変更を導入します。

手順については、次を参照してください。

Firewall Threat Defense デバイスについては、Cisco Secure Firewall Management Center デバイス構成ガイドの「*Configure NTP Time Synchronization for Threat Defense*」を参照してください。

時刻同期の設定の変更について

- Firewall Management Center とその管理対象デバイスは正確な時刻に大きく依存しています。システムクロックは、システムの時刻を維持するシステム機能です。システムクロックは協定世界時（UTC）に設定されています。これは、時計と時刻を管理するために世界で使用されている基本的な標準時間です。

  システム時刻を変更しようとしないでください。システムタイムゾーンの UTC からの変更はサポートされていません。また、システムタイムゾーンを変更した場合はデバイスを再イメージ化してサポートされていない状態から回復させる必要があります。

- NTP を使用して時刻を提供するように Firewall Management Center を設定してから、後でそれを無効にした場合、管理対象デバイスの NTP サービスは引き続き Firewall Management Center と時刻を同期しようとします。新しい時刻ソースを確立するには、すべての該当するプラットフォーム設定ポリシーを更新および再展開する必要があります。

- Firewall Management Center を NTP サーバーとして設定後、時刻を手動で変更するには、NTP オプションを無効にして時刻を手動で変更してから NTP オプションを再度有効にします。

UCAPL/CC コンプライアンス

お客様の組織が、米国防総省およびグローバル認定組織によって確立されたセキュリティ基準に従う機器とソフトウェアだけを使用することを求められる場合があります。この設定の詳細については、セキュリティ認定準拠のモードを参照してください。

構成のアップグレード

ポリシー属性、オブジェクト、またはその他のデバイス設定は、Firewall Management Center のアップグレードの一部として変更される場合があります。Firewall Management Center をメジャーバージョンにアップグレードすると、特定の機能がデフォルトで有効になる場合があります。[構成のアップグレード（Upgrade Configuration）] 設定を使用すると、Firewall Management Center の次のメジャーバージョンへのアップグレードを完了したときに、保留中の設定変更のレポートを生成できます。このレポートには、アップグレード後に管理対象デバイスへの展開が保留されているポリシーおよびデバイス設定の変更が表示されます。Firewall Management Center のアップグレードが完了したら、**[Message Center]** > **[タスク（Tasks）]** を選択してレポートをダウンロードします。

保留中の設定変更のレポートには、次のものが含まれます。

- **比較ビュー**：管理対象デバイスへの展開が保留されている、アップグレード後のすべての設定変更を、現在のデバイス設定と比較します。
- **詳細ビュー**：CLI を使用して、保留中の設定変更をプレビューできます。

保留中の設定変更に関するレポートの詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドの「*Deployment Preview*」を参照してください。

アップグレード後のレポートの有効化

Firewall Management Center のメジャー バージョン アップグレード後に管理対象デバイスに展開される保留中のすべての設定変更に関するレポートを生成します。

手順

ステップ 1 [システム（System）]（⚙）> **[構成（Configuration）]** を選択します。

ステップ 2 [アップグレード後レポートの有効化（Enable Post-Upgrade Report）] チェックボックスをオンにして、このオプションを有効にします。

レポートは、Firewall Management Center の次のメジャー バージョン アップグレード後に生成されます。このオプションは、アップグレード後にすべての管理対象デバイスのレポートを生成します。レポートの生成に必要な時間は、設定のサイズと管理対象デバイスの数によって異なります。

ステップ 3 [保存（Save）] をクリックします。

ユーザーの設定

グローバルユーザーの設定は、Firewall Management Centerのすべてのユーザーに影響します。[User Configuration] ページで次の設定を行います（[システム（System）]（⚙） > **[構成（Configuration）] > [ユーザー構成（User Configuration）]**）。

- [パスワード再使用制限（Password Reuse Limit）]：ユーザーの最新の履歴の中で再利用できないパスワードの数。この制限は、すべてのユーザーの Web インターフェイスに適用されます。`admin` ユーザーの場合、これは CLI アクセスにも適用されます。システムは各アクセス形式に対して個別のパスワード リストを維持します。制限をゼロに設定すると（デフォルト）パスワードの再利用に制限は課せられません。パスワードの再使用制限の設定 （93 ページ）を参照してください。

- [成功したログインの追跡（Track Successful Logins）]：Firewall Management Center へのログインの成功をユーザーごとにアクセス方式（Web インターフェイスまたは CLI）別に追跡する日数。ユーザーがログインすると、使用しているインターフェイスで成功したログイン回数が表示されます。[成功したログインの追跡（Track Successful Logins）] をゼロに設定すると（デフォルト）、システムは成功したログインアクティビティを追跡せず、レポートもしません。成功したログインの追跡 （94 ページ）を参照してください。

- [ログイン失敗の最大数（Max Number of Login Failures）]：ユーザーが誤った Web インターフェイスのログインクレデンシャルを連続して入力できる回数。この回数を超えると、設定されている時間にわたって一時的にアカウントにアクセスできなくなります。一時的なロックアウトが適用されている間にユーザーがログインを試行し続けた場合：

  - 一時的なロックアウトが適用されていることをユーザーに通知せず、（有効なパスワードを使用したとしても）システムはそのアカウントへのアクセスを拒否します。
  - ログイン試行のたびにシステムはそのアカウントの失敗ログイン数を増やし続けます。
  - ユーザーが個人の [ユーザー設定（User Configuration）] ページでそのアカウントに設定した [ログイン失敗の最大数（Maximum Number of Failed Logins）] を超えた場合、管理者ユーザーがそのアカウントを再アクティブ化するまではそのアカウントはロックアウトされます。

- [一時的にユーザーをロックアウトする分単位の時間の設定（Set Time in Minutes to Temporarily Lockout Users）]：[ログイン失敗の最大数（Max Number of Failed Logins）] がゼロ以外の場合にユーザーが一時的に Web インターフェイスからロックアウトされる分単位の時間。

- **許可された最大同時セッション数**

  - ユーザーの最大セッション数：同時に開くことができる特定のタイプ（読み取り専用または読み取り/書き込み）のセッション数。セッションのタイプは、ユーザーに割り当てられたロールによって決定されます。ユーザーに読み取り専用ロールのみが割り当てられている場合、そのユーザーのセッションは、[（読み取り専用）（(Read Only)）]セッションの制限に対してカウントされます。ユーザーが書き込み権限があ

るロールを持っている場合、セッションは、[読み取り/書き込み（Read/Write）] セッションの制限に対してカウントされます。たとえば、ユーザーにAdminロールが割り当てられていて、[読み取り/書き込み権限を持つユーザーおよびCLIユーザーの最大セッション数（Maximum sessions for users with Read/Write privileges/CLI users）] が 5 に設定されている場合、読み取り/書き込み権限を持つ5人の他のユーザーがすでにログインしていると、そのユーザーはログインできません。

（注） システムが同時セッション制限の目的で読み取り専用と見なす定義済みユーザーロールおよびカスタムユーザーロールには、[システム（System）]（⚙）>**[ユーザー（Users）]**>**[ユーザー（Users）]** と [システム（System）]（⚙）>**[ユーザー（Users）]**>**[ユーザーロール（User Roles）]** にあるロール名に [(Read Only)] というラベルが付けられます。ユーザー ロールのロール名に [（読み取り専用）（(Read Only)）] が含まれていない場合、システムはそのロールを読み取り/書き込みと見なします。システムは、必要な条件を満たすロールに [（読み取り専用）（(Read Only)）] を自動的に適用します。読み取り専用のテキスト文字列をロール名に手動で追加してロールを読み取り専用にすることはできません。

セッションのタイプごとに、最大制限を 1 ～ 1024 の範囲で設定できます。[許可された最大同時セッション数（Max Concurrent Sessions Allowed）] がゼロ（デフォルト）に設定されている場合、同時セッション数は無制限になります。

同時セッションの制限をより限定的な値に変更しても、システムは現在開いているセッションを閉じません。ただし、指定された数を超えて新しいセッションが開かれないようにします。

- [IPアドレスごとの最大同時接続数（Maximum concurrent connections per IP Address）]：1 つの IP アドレスから同時に開くことができる Web サーバーの同時接続数。デフォルトでは、IP アドレスあたりの最大同時接続数は 50 に制限されています。最大数は 20 ～ 100 の範囲で設定できます。

（注） IP アドレスあたりの最大同時セッション数を増やすと、Firewall Management Center のパフォーマンスが低下する可能性があります。

パスワードの再使用制限の設定

[パスワード再利用の制限（Password Reuse Limit）] を有効にすると、システムに Firewall Management Center ユーザーの暗号化されたパスワード履歴が保持されます。ユーザーはパスワード履歴内のパスワードを再利用できません。各ユーザーの保存されたパスワードの数をア

クセス方式（Webインターフェイスまたは CLI）ごとに指定できます。ユーザーの現在のパスワードはこの番号に対してカウントされます。制限を低くすると、システムは履歴から古い順にパスワードを削除します。制限を高くすると、削除されたパスワードが復元されません。

手順

ステップ 1 [システム（System）]（⚙）> **[構成（Configuration）]** を選択します。

ステップ 2 [User Configuration] をクリックします。

ステップ 3 [Password Reuse Limit] を履歴に維持したいパスワードの数（最大 256）に設定します。

パスワード再利用のチェックを無効にするには、0 を入力します。

ステップ 4 [保存（Save）] をクリックします。

成功したログインの追跡

この手順を使用して、各ユーザーの成功したログインの追跡を指定した日数の間、有効にします。この追跡が有効になっている場合は、ユーザーがWebインターフェイスまたはCLIにログインしたときにシステムは成功したログイン数を表示します。

（注） 日数を少なくすると、システムはログインのレコードを古いものから削除します。制限値を大きくすると、システムはその日数からカウントを復元しません。その場合、成功したログインの復元された数は、一時的に実際の番号よりも少なくなる場合があります。

手順

ステップ 1 [システム（System）]（⚙）> **[構成（Configuration）]** を選択します。

ステップ 2 [User Configuration] をクリックします。

ステップ 3 [成功したログイン日数の追跡（Track Successful Login Days）] を成功したログインを追跡する日数（最大 365）に設定します。

ログインの追跡を無効にするには、0 を入力します。

ステップ 4 [保存（Save）] をクリックします。

一時的なロックアウトの有効化

システムがロックアウトを有効にする前に連続して失敗したログイン試行を許可する回数を指定して、一時的な時限ロックアウト機能を有効にします。

手順

ステップ 1 [システム（System）]（⚙）>**[構成（Configuration）]** を選択します。

ステップ 2 [User Configuration] をクリックします。

ステップ 3 [ログイン失敗の最大数（Max Number of Login Failures）] をユーザーが一時的にロックアウトされるまで連続して失敗できるログイン試行の最大回数に指定します。

一時的なロックアウトを無効にするには、ゼロを入力します。

ステップ 4 [ユーザーを一時的にロックアウトする分単位の時間（Time in Minutes to Temporarily Lockout Users）] は一時的なロックアウトをトリガーしたユーザーをロックアウトする分数に設定します。

この値がゼロの場合は、[ログイン失敗最大数（Max Number of Login Failures）] がゼロ以外でも、ユーザーはログインの再試行を待機する必要はありません。

ステップ 5 [保存（Save）] をクリックします。

同時セッションの最大数の設定

同時に開くことができる特定のタイプ（読み取り専用または読み取り/書き込み）のセッションの最大数を指定できます。セッションのタイプは、ユーザーに割り当てられたロールによって決定されます。ユーザーに読み取り専用ロールのみが割り当てられている場合、そのユーザーのセッションは、[（読み取り専用）（(Read Only)）] セッションの制限に対してカウントされます。ユーザーが書き込み権限があるロールを持っている場合、セッションは、[読み取り/書き込み（Read/Write）] セッションの制限に対してカウントされます。

手順

ステップ 1 [システム（System）]（⚙）>**[構成（Configuration）]** を選択します。

ステップ 2 [User Configuration] をクリックします。

ステップ 3 セッションのタイプごとに、**[許可された最大同時セッション数（Max Concurrent Sessions Allowed）]** をそのタイプのセッションの最大数（同時に開くことができる）に設定します。

ユーザーごとの同時セッションの制限を適用しない場合は、0 を入力します。

（注）

同時セッションの制限をより限定的な値に変更しても、システムは現在開いているセッションを閉じません。ただし、指定された数を超えて新しいセッションが開かれないようにします。

ステップ 4 [保存（Save）] をクリックします。

VMware ツール

VMware Tools は、仮想マシン向けのパフォーマンスを向上させるためのユーティリティ スイートです。これらのユーティリティを使用すると、VMware 製品の便利な機能をすべて活用できます。VMware で実行されている Cisco Secure Firewall 仮想アプライアンスは、次のプラグインをサポートします。

- guestInfo
- powerOps
- timeSync
- vmbackup

サポートされるすべてのバージョンの ESXi で VMware Tools を有効にすることもできます。VMware Tools のすべての機能については、VMware の Web サイト（http://www.vmware.com/）を参照してください。

VMware 向け Secure Firewall Management Center での VMware ツールの有効化

手順

ステップ 1 [システム（System）]（⚙）>**[構成（Configuration）]**を選択します。
ステップ 2 [VMware ツール（VMware Tools）] をクリックします。
ステップ 3 [VMware ツールの有効化（Enable VMware Tools）] をクリックします。
ステップ 4 [保存（Save）] をクリックします。

脆弱性マッピング

サーバーのディスカバリ イベント データベースにアプリケーション ID が含まれており、トラフィックのパケットヘッダーにベンダーおよびバージョンが含まれる場合、システムは、その

アドレスから送受信されるすべてのアプリケーション プロトコル トラフィックについて、脆弱性をホスト IP アドレスに自動的にマップします。

パケットにベンダー情報もバージョン情報も含まれないサーバすべてに対して、システムでこれらのベンダーとバージョンレスのサーバのサーバ トラフィックと脆弱性を関連付けるかどうかを設定できます。

たとえば、ホストがヘッダーにベンダーまたはバージョンが含まれていないSMTP トラフィックを提供しているとします。システム設定の [脆弱性マッピング（Vulnerability Mapping）] ページでSMTP サーバを有効にしてから、そのトラフィックを検出するデバイスを管理するFirewall Management Center にその設定を保存した場合、SMTP サーバと関連付けられているすべての脆弱性がそのホストのホスト プロファイルに追加されます。

ディテクタがサーバー情報を収集して、それをホスト プロファイルに追加しますが、アプリケーション プロトコル ディテクタは脆弱性のマッピングに使用されません。これは、カスタム アプリケーション プロトコル ディテクタにベンダーまたはバージョンを指定できず、また脆弱性マッピング用のサーバーを選択できないためです。

サーバの脆弱性のマッピング

この手順には、スマートライセンス。

手順

ステップ 1 [システム（System）]（⚙）> **[構成（Configuration）]**を選択します。

ステップ 2 [脆弱性マッピング（Vulnerability Mapping）] を選択します。

ステップ 3 次の選択肢があります。

- ベンダーまたはバージョンの情報が含まれていないアプリケーション プロトコル トラフィックを受信するホストに、サーバの脆弱性がマップされないようにするには、そのサーバのチェックボックスをオフにします。
- ベンダーまたはバージョンの情報が含まれていないアプリケーション プロトコル トラフィックを受信するホストに、サーバの脆弱性がマップされるようにするには、そのサーバのチェックボックスをオフにします。

ヒント
[有効（Enabled）] の横にあるチェックボックスを使用すると、すべてのチェックボックスを一度にオンまたはオフにできます。

ステップ 4 [保存（Save）] をクリックします。

Web 分析

デフォルトでは、ファイアウォール製品の向上のために、ページの閲覧内容、ブラウザのバージョン、製品バージョン、ユーザーの場所、Firewall Management Center アプライアンスの管理IPアドレスまたはホスト名など、個人を特定できない使用データがシスコによって収集されます。

データ収集は、エンドユーザー ライセンス契約書に同意した後に開始されます。このデータの継続的な収集を拒否する場合は、次の手順を実行してオプト アウトできます。

手順

ステップ 1 [システム（System）]（⚙）>**[設定（Configuration）]**を選択します。
ステップ 2 [Web 分析（Web Analytics）] をクリックします。
ステップ 3 適切に選択してから、[保存（Save）] をクリックします。

次のタスク

（オプション）シスコへの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 （9 ページ）を参照してください。

システム設定の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
高度な脅威ハンティングとインテリジェンス収集に向けた Cisco Talos の有効化	7.6.0	任意（Any）	Cisco Talos が脅威の状況をより包括的に理解し、より優れた保護戦略を確立することを支援できるようになりました。**[システム]** > **[設定（Configuration）]** > **[侵入ポリシーの設定（Intrusion Policy Preferences）]** をクリックし、**[Talos 脅威ハンティングテレメトリ（Talos Threat Hunting Telemetry）]** チェックボックスをオンにして、Talos がグローバル侵入ポリシーに特別な IPS ルールセットを含めることを許可します。これらのルールにより、Talos は高度な脅威ハンティングを実行し、これらの脅威分析とインテリジェンス収集のためのルールによってトリガーされたイベントを収集できます。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
アップグレード後のレポートの有効化	7.4.1	任意	Secure Firewall Management Center の次のメジャー バージョン アップグレード後に、管理対象デバイスに展開される保留中の設定変更のレポートを生成することを選択できるようになりました。 新規/変更された画面：**[システム（System）] > [設定（Configuration）] > [設定のアップグレード（Upgrade Configuration）]**。 必要最低限の Threat Defense：任意
アクセス制御のパフォーマンスの向上（オブジェクトの最適化）。	7.2.4 7.4.0	任意（Any）	**アップグレードの影響。7.2.4 ～ 7.2.5 または 7.4.0 への Firewall Management Center アップグレード後の最初の展開には時間がかかり、デバイスの CPU 使用率が高くなる可能性があります。** アクセス コントロール オブジェクトの最適化により、ネットワークが重複するアクセス コントロール ルールがある場合、パフォーマンスが向上し、デバイスリソースの消費が少なくなります。最適化は、Management Center で機能が有効になった後の最初の展開時に管理対象デバイスで行われます（アップグレードで有効になった場合も含む）。ルールの数が多い場合、システムがポリシーを評価してオブジェクトの最適化を実行するのに数分から 1 時間かかることがあります。この間、デバイスの CPU 使用率も高くなることがあります。機能が無効になった後の最初の展開でも同様のことが発生します（アップグレードによって無効になった場合も含む）。この機能が有効または無効になった後は、メンテナンス時間帯やトラフィックの少ない時間帯など、影響が最小限になる時間に展開することを強く推奨します。 新規/変更された画面（バージョン 7.2.6/7.4.1 が必要）：**[システム（System）] > [設定（Configuration）] > [アクセス制御の設定（Access Control Preferences）] > [オブジェクトグループの最適化（Object-group optimization）]**。 バージョンの制限：Firewall Management Center バージョン 7.3.x ではサポートされていません。
監査ログの設定変更。	7.4	いずれか	設定データの形式とホストを指定することにより、設定変更を監査ログデータの一部として syslog にストリーミングできます。Management Center は、監査構成ログのバックアップと復元をサポートしています。この機能は、Management Center の高可用性設定でもサポートされています。 新規/変更された画面：**[システム（System）] > [設定（Configuration）] > [監査ログ（Audit Log）]**

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
フランス語オプション。	7.2	任意（Any）	Management Center の Web インターフェイスをフランス語に切り替えることができるようになりました。 新規/変更された画面：**[システム（System）] > [設定（Configuration）] > [言語（Language）]**。
ほとんどの接続イベントをイベントレート制限から除外します。	7.0	任意（Any）	接続データベースの [最大接続イベント数（Maximum Connection Events）] の値を 0 に設定すると、優先順位の低い接続イベントが FMC ハードウェアのフローレート制限にカウントされなくなります。以前は、この値を 0 に設定すると、イベントストレージにのみ適用され、フローレート制限には影響しませんでした。 新規/変更された画面：**[システム（System）] > [設定（Configuration）] > [データベース（Database）]**。 サポートされているプラットフォーム：ハードウェア FMC。
NTP サーバーの AES-128 CMAC 認証のサポート。	7.0	任意（Any）	FMC と NTP サーバー間の接続は、AES-128 CMAC キーと、以前にサポートされていた MD5 キーおよび SHA-1 キーを使用して保護できます。 新規/変更された画面：**[システム（System）] > [設定（Configuration）] > [時刻の同期（Time Synchronization）]**
サブジェクト代替名（SAN）。	6.6	任意（Any）	FMC の HTTPS 証明書を作成するときに、SAN フィールドを指定できます。証明書が複数のドメイン名または IP アドレスを保護する場合は、SAN を使用することを推奨します。SAN の詳細については、RFC 5280、セクション 4.2.1.6 を参照してください。 新規/変更された画面：**[システム（System）] > [設定（Configuration）] > [HTTPS証明書（HTTPS Certificate）]**
HTTPS 証明書。	6.6	任意（Any）	現在、システムとともに提供されるデフォルトの HTTPS サーバークレデンシャルは 800 日で期限が切れます。バージョン 6.6 にアップグレードする前に生成されたデフォルトの証明書がアプライアンスで使用されている場合、証明書の有効期限は、証明書が生成されたときに使用されていた Firepower バージョンによって異なります。詳細については、デフォルト HTTPS サーバー証明書 （37 ページ）を参照してください。 サポートされているプラットフォーム：ハードウェア FMC。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
NTP の保護。	6.5	任意（Any）	FMC は、SHA1 または MD5 対称キー認証を使用して NTP サーバーとのセキュア通信をサポートしています。 新規/変更された画面：**[システム（System）] > [設定（Configuration）] > [時刻の同期（Time Synchronization）]**
Web 解析。	6.5	任意（Any）	Web 分析データの収集は、EULA に同意した後に開始されます。以前と同様に、データの共有を停止することを選択できます。Web 分析（98 ページ）を参照してください。
FMC の自動 CLI アクセス。	6.5	任意（Any）	SSH を使用して FMC にログインすると、CLI に自動的にアクセスします。CLI `expert` コマンドを使用して Linux シェルにアクセスすることもできますが、このコマンドを使用しないことを強く推奨します。 （注） FMC の CLI アクセスを有効または無効にするバージョン 6.3 の機能は廃止されます。このオプションが廃止された結果、仮想 FMC には **[システム（System）] > [設定（Configuration）] > [コンソール設定（Console Configuration）]**ページは表示されなくなりました。このページは、物理 FMC では引き続き表示されます。
読み取り専用および読み取り/書き込みアクセスに設定可能なセッション制限。	6.5	任意（Any）	[許可された最大同時セッション数（Max Concurrent Sessions Allowed）] の設定が追加されました。この設定により、管理者は同時に開くことができる特定のタイプ（読み取り専用または読み取り/書き込み）のセッションの最大数を指定できます。 （注） システムが同時セッション制限の目的で読み取り専用と見なす定義済みユーザーロールおよびカスタムユーザーロールには、**[システム（System）] > [ユーザー（Users）] > [ユーザー（Users）]** および **[システム（System）] > [ユーザー（Users）] > [ユーザーロール（User Roles）]** にあるロール名に **[（読み取り専用）（(Read Only)）]** というラベルが付けられます。ユーザー ロールのロール名に [（読み取り専用）（(Read Only)）] が含まれていない場合、システムはそのロールを読み取り/書き込みと見なします。 新規/変更された画面： • **[システム（System）] > [設定（Configuration）] > [ユーザー設定（User Configuration）]** • **[システム（System）] > [ユーザー（Users）] > [ユーザー ロール（User Roles）]**

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
管理インターフェイスで重複アドレス検出（DAD）を無効にする機能。	6.4	任意（Any）	IPv6 を有効にすると、DAD を無効にすることができます。DAD を使用することによってサービス拒否攻撃の可能性が拡大するため、DAD は無効にすることができます。この設定を無効にした場合は、すでに割り当てられているアドレスがこのインターフェイスで使用されていないことを手動で確認する必要があります。 新規/変更された画面：**[システム（System）] > [設定（Configuration）] > [管理インターフェイス（Management Interfaces）] > [インターフェイス（Interfaces）] > [インターフェイスの編集（Edit Interface）] > [IPv6 DAD]** サポート対象プラットフォーム: FMC
管理インターフェイス上の ICMPv6 エコー応答および宛先到達不能メッセージを無効にする機能。	6.4	任意（Any）	IPv6 を有効にすると、ICMPv6 エコー応答および宛先到達不能メッセージを無効できるようになりました。これらのパケットを無効にすることで、サービス拒否攻撃の可能性から保護します。エコー応答パケットを無効にすると、デバイスの管理インターフェイスにテスト目的で IPv6 ping を使用できなくなります。 新規/変更された画面：**[システム（System）] > [設定（Configuration）] > [ICMPv6]** 新規/変更されたコマンド：**configure network ipv6 destination-unreachable**、**configure network ipv6 echo-reply** サポートされているプラットフォーム：FMC（Web インターフェイスのみ）、FTD（CLI のみ）

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
グローバルユーザー構成設定。	6.3	任意（Any）	[成功したログインの追跡（Track Successful Logins）]の設定を追加しました。システムは、選択した日数までに各 FMC アカウントで実行され、成功したログインの回数を追跡できます。この機能を有効にすると、ログイン中のユーザーには、設定した過去の日数内にシステムへのログインが何回成功したかを報告するメッセージが表示されます（Web インターフェイスとシェル/CLI アクセスに適用）。 [パスワード再利用制限（Password Reuse Limit）] の設定を追加しました。設定可能な過去のパスワード数について各アカウントのパスワードの履歴を追跡できます。システムは、すべてのユーザーがその履歴に表示されているパスワードを再利用できないようにします（Web インターフェイスとシェル/CLI アクセスに適用）。 [ログイン失敗の最大数（Max Number of Login Failures）] と [ユーザーを一時的にロックアウトする分単位の時間の設定（Set Time in Minutes to Temporarily Lockout Users）] の設定を追加しました。これらの機能によって、管理者はシステムが設定可能な時間にわたってアカウントを一時的にブロックするまでに、ユーザーが誤った Web インターフェイスのログインクレデンシャルを連続して入力できる回数を制限できます。 新規/変更された画面：**[システム（System）] > [設定（Configuration）] > [ユーザー設定（User Configuration）]** サポート対象プラットフォーム: FMC
HTTPS 証明書。	6.3	任意（Any）	現在、システムとともに提供されるデフォルトの HTTPS サーバー クレデンシャルは 3 年で期限が切れます。バージョン 6.3 にアップグレードされる前に生成されたデフォルトのサーバー証明書をアプライアンスが使用している場合、サーバー証明書は最初に生成されたときから 20 年後に期限切れとなります。デフォルトの HTTPS サーバー証明書を使用している場合、システムはその証明書を更新する機能を提供しています。 新規/変更された画面：**[システム（System）] > [設定（Configuration）] > [HTTPS証明書（HTTPS Certificate）] > [HTTPS証明書の更新（Renew HTTPS Certificate）]**。 サポート対象プラットフォーム: FMC

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
FMC の CLI アクセスを有効化および無効化する機能。	6.3	任意（Any）	FMC の Web インターフェイスで管理者が使用可能な新しいチェックボックス：**[システム（System）]**>**[設定（Configuration）]**>**[コンソール設定（Console Configuration）]** の **[CLIアクセスの有効化（Enable CLI Access）]**。 • オン： SSH を使用して FMC にログインすると CLI にアクセスします。 • オフ：SSH を使用して FMC にログインすると Linux シェルにアクセスします。これは、バージョン 6.3 の新規インストールと、以前のリリースからバージョン 6.3 にアップグレードした場合のデフォルトの状態です。 バージョン 6.3 より前では、[コンソール設定（Console Configuration）] ページには 1 つの設定のみしかなく、物理デバイスのみに適用されていました。そのため、[コンソール設定（Console Configuration）] ページは仮想 FMC では使用できませんでした。この新しいオプションを追加することで、[コンソール設定（Console Configuration）] ページに物理 FMC とともに 仮想 FMC が表示されるようになりました。ただし、仮想 FMC の場合、このページに表示されるのはこのチェックボックスのみです。 サポート対象プラットフォーム: FMC

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。