



従来型デバイス用の Firepower プラットフォーム設定

次のトピックでは、Firepower プラットフォーム設定について、および従来型デバイスでそれを設定する方法について説明します。

- [Firepower プラットフォーム設定の概要, 1 ページ](#)
- [Firepower プラットフォームの設定, 2 ページ](#)
- [アクセスリスト, 3 ページ](#)
- [監査ログ, 4 ページ](#)
- [外部認証の設定, 7 ページ](#)
- [言語の選択, 9 ページ](#)
- [ログインバナー, 11 ページ](#)
- [セッションタイムアウト, 12 ページ](#)
- [SNMP ポーリング, 14 ページ](#)
- [STIG コンプライアンス, 16 ページ](#)
- [時刻および時刻同期, 18 ページ](#)

Firepower プラットフォーム設定の概要

Firepower クラシック管理対象デバイス向けのプラットフォーム設定は無関係な機能の範囲を指定しますが、その値は複数のデバイス間で共有できます。この場合は、7000および8000シリーズ、ASA FirePOWER モジュールやNGIPSv デバイスです。デバイスごとに異なる設定を使用する場合でも、共有ポリシーを作成して目的のデバイスに適用する必要があります。

関連トピック

[管理対象デバイス用のプラットフォーム設定ポリシー](#)

システム設定

Firepower プラットフォームの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	従来型 (Classic)	任意 (Any)	Admin

プラットフォームを設定するには、既存のプラットフォーム設定ポリシーを編集するか、新しいポリシーを作成します。デバイスに現在展開されているプラットフォーム設定ポリシーを編集する場合、変更を保存した後にポリシーを再展開してください。

手順

ステップ 1 [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択します。既存のシステム ポリシーのリストを含む、[プラットフォーム設定 (Platform Settings)] ページが表示されます。

ステップ 2 新しいポリシーを作成するか、既存のポリシーを編集します。

- 新しいポリシーを作成するには、[プラットフォーム設定ポリシーの作成](#)を参照してください。
- 既存のポリシーを編集するには、そのポリシーの横にある編集アイコン (✎) をクリックします。

[ポリシーの編集 (Edit Policy)] ページが表示されます。ポリシー名とポリシーの説明を変更できます。プラットフォーム設定ポリシーのそれぞれの側面の設定については、次の項のいずれかを参照してください。

- [システムのアクセス リストの設定](#)
- [外部ストリーミングの監査ログの設定](#)
- [外部認証の有効化, \(8 ページ\)](#)
- [別の言語の指定](#)
- [カスタム ログイン バナーの追加](#)
- [セッションタイムアウトの設定](#)
- [SNMP ポーリングの設定](#)
- [STIG コンプライアンスの有効化](#)

- [Firepower Management Center からの時間の提供](#)

- ステップ 3** (オプション) [ポリシー割り当て (Policy Assignment)] をクリックして、ポリシーを展開する利用可能なデバイスを選択します。[ポリシーに追加 (Add to Policy)] をクリックして (またはドラッグアンドドロップして)、選択したデバイスを追加します。
[検索 (Search)] フィールドに検索文字列を入力して、デバイスのリストを絞り込むことができます。
- ステップ 4** [保存 (Save)] をクリックします。

次の作業

- 設定変更を展開します。[設定変更の導入](#)を参照してください。

アクセス リスト

Firepower Management Center およびクラシック管理対象デバイスでは、アクセスリストを使用して、IP アドレスとポートを基準にシステム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) : コマンドライン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。



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。

システムのアクセス リストの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center 従来型 (Classic)	任意 (Any)	Admin

この構成は、Firepower Management Center または従来の管理対象デバイス (7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv) に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来型の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、構成は、システム構成変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで有効になりません。

このアクセス リストは、外部データベース アクセスを制御しないので注意してください。

手順

-
- ステップ 1** Firepower Management Center を構成するか従来の管理対象デバイスを構成するかに応じて、次の操作を実行します。
- Management Center : [システム (System)] > [設定 (Configuration)] を選択します。
 - 管理対象デバイス : [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower ポリシーを作成または編集します。
- ステップ 2** [アクセス リスト (Access List)] をクリックします。
- ステップ 3** 現在の設定の 1 つを削除するために、削除アイコン (🗑️) をクリックすることもできます。
注意 アプライアンスのインターフェイス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、IP=any port=443 のエントリが存在しない場合、ポリシーを展開した時点でシステムへのアクセスは失われます。
- 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。
-

次の作業

- 設定変更を展開します。 [設定変更の導入](#) を参照してください。

監査ログ

Firepower Management Center および従来型管理対象デバイスは、ユーザ アクティビティに関する読み取り専用の監査情報をログに記録します。Management Center および 7000 および 8000 シリーズの Web インターフェイスでは、監査ログ イベントは標準イベント ビューに表示されます。標

準イベントビューでは、監査ビューの任意の項目に基づいて監査ログメッセージの表示、並べ替え、フィルタ処理ができます。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。

監査ログメッセージを `syslog` に送信するよう、Firepower Management Center および従来型管理対象デバイスを設定することもできます。設定するには、`syslog` サーバ、およびメッセージに関連付ける重大度、ファシリティ、オプションタグを指定します。タグは、`syslog` の監査ログメッセージと一緒に表示されます。ファシリティはメッセージを作成するサブシステムを示し、重大度はメッセージの重大度を定義します。`syslog` メッセージにはファシリティおよび重大度は含まれません。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す値です。

また、監査ログメッセージを HTTP サーバにストリーミングするよう、Firepower Management Center および従来型管理対象デバイスで設定することもできます。

監査ログストリーミング設定は、アプライアンスのタイプによって異なる設定の一部となっています。

- Firepower Management Center では、監査ログのストリーミングはシステム設定の一部です。
- クラシック管理対象デバイスでは、監査ログストリーミングは Firepower Management Center プラットフォーム設定ポリシーの一部です。

いずれの場合も、システム設定の変更を保存するか、共有プラットフォーム設定ポリシーを展開するまでは設定は有効になりません。

外部ストリーミングの監査ログの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center 従来型 (Classic)	任意 (Any)	Admin

この構成は、Firepower Management Center または従来の管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv）に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、構成は、システム構成変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで有効になりません。

次に、出力構造の例を示します。

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

現地の日付、時刻、およびホスト名の後に、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。

次に例を示します。

```
Mar 01 14:45:24 localhost [TAG] Dev-DC3500: admin@10.1.1.2, Operations > Monitoring, Page View
```

はじめる前に

- 外部ホストが機能していることと、監査ログを送信するシステムからアクセスできることを確認します。

手順

-
- ステップ 1** Firepower Management Center を構成するか従来の管理対象デバイスを構成するかに応じて、次の操作を実行します。
- Management Center : [システム (System)] > [設定 (Configuration)] を選択します。
 - 管理対象デバイス : [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択して、Firepower ポリシーを作成または編集します。
- 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** [ホスト (Host)] フィールドにあるホストの IP アドレスまたは完全修飾名を使用して、監査情報の宛先ホストを指定します。デフォルトポート (514) が使用されます。
- 注意** 監査ログを受け入れるように設定しているコンピュータが、リモートメッセージを受け入れるようにセットアップされていない場合、ホストは監査ログを受け入れません。
- ステップ 5** [syslog ファシリティ (syslog Facility)] を選択します。
- ステップ 6** 重大度を選択します。
- ステップ 7** 必要に応じて、[タグ (オプション) (Tag (optional))] フィールドで参照タグを挿入します。
- ステップ 8** 定期的な監査ログの更新を外部 HTTP サーバに送信するには、[監査ログを HTTP サーバに送信 (Send Audit Log to HTTP Server)] ドロップダウンリストから [有効化 (Enabled)] を選択します。
- ステップ 9** [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。次にリストされている HTTP POST 変数を要求するリスナープログラムに対応する URL を入力する必要があります。
- subsystem
 - actor
 - event_type
 - message

- action_source_ip
- action_destination_ip
- 結果
- 時刻
- tag (上記のように定義されている場合)

注意 暗号化されたポストを許可するには、HTTPS URL を使用する必要があります。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。

ステップ 10 [保存 (Save)] をクリックします。

次の作業

- 設定変更を展開します。[設定変更の導入](#)を参照してください。

外部認証の設定

外部認証サーバを参照する認証オブジェクトを作成する場合、外部認証を有効にすることにより、ローカル データベースを使用せずに、管理対象デバイスにログインしているユーザをそのサーバに認証させることができます。

外部認証を有効にすると、システムではLDAPまたはRADIUSサーバのユーザのユーザクレデンシャルが確認されます。さらに、ユーザがローカルの内部認証を有効にしており、ユーザクレデンシャルが内部データベースにない場合、システムは一致するクレデンシャルのセットがないか外部サーバを検査します。ユーザが複数のシステムで同じユーザ名を持っている場合、すべてのサーバですべてのパスワードが動作します。ただし、使用可能な外部認証サーバで認証が失敗した場合、システムはローカル データベースの検査に戻らないので注意してください。

外部認証を有効にすると、アカウントが外部で認証されている任意のユーザのデフォルトのユーザ ロールを設定できます。これらのロールを組み合わせたことができる場合は、複数のロールを選択できます。たとえば、自社の [ネットワーク セキュリティ (Network Security)] グループのユーザのみを取得する外部認証を有効にした場合、デフォルトのユーザ ロールを設定して [セキュリティ アナリスト (Security Analyst)] ロールを組み込み、ユーザが自分で追加のユーザ設定を行わなくても収集されたイベント データにアクセスできるようにすることが可能です。ただし、外部認証がセキュリティ グループに加えて他のユーザのレコードを取得する場合、デフォルトのロールを未選択のままにしておきたい場合もあります。

アクセス ロールが選択されていない場合、ユーザはログインできますが、どの機能にもアクセスできません。ユーザがログインを試行すると、アカウントがユーザ管理ページ ([システム (System)] > [ユーザ (Users)]) に表示されます。ここで、追加の権限を付与するアカウント設定を編集できます。

**ヒント**

1つのユーザロールを使用するようにシステムを設定してそのポリシーを適用し、後で設定を変更して別のデフォルトのユーザロールを使用する場合、アカウントを変更するか、削除して再作成するまで、変更前に作成されたユーザアカウントはすべて、最初のユーザロールを保持します。

シェルアクセスまたはCAC認証および承認のためにLDAPサーバに対して認証できる一連のユーザを指定する場合は、それぞれに個別の認証オブジェクトを作成し、オブジェクトを個別に有効にする必要があります。

内部認証によってユーザがログインしようとする時、システムは最初にそのユーザがローカルユーザデータベースに存在するかどうかを検査します。ユーザが存在する場合、システムは次にユーザ名とパスワードをローカルデータベースに対して検査します。一致が検出されると、ユーザは正常にログインします。ただし、ログインが失敗し、外部認証が有効になっている場合、システムはそれぞれの外部認証サーバに対して、ユーザを設定に表示される認証順序で検査します。ユーザ名およびパスワードが外部サーバからの結果と一致した場合、システムはユーザを、その認証オブジェクトに対してデフォルトの権限を持つ外部ユーザに変更します。

外部ユーザがログインしようとする時、システムは外部認証サーバに対してユーザ名およびパスワードを検査します。一致が検出されると、ユーザは正常にログインします。ログインが失敗した場合、ユーザのログイン試行は拒否されます。外部ユーザは、ローカルデータベース内のユーザリストに対して認証できません。ユーザが新しい外部ユーザの場合、外部認証オブジェクトのデフォルト権限を持つ外部ユーザアカウントがローカルデータベースに作成されます。

関連トピック

[ユーザアカウント](#)

外部認証の有効化

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center、従来型	任意 (Any)	Admin

はじめる前に

- [外部認証 \(External Authentication\)](#) の説明に従って外部認証オブジェクトを設定します。

手順

- ステップ 1 [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower ポリシーを作成または編集します。
- ステップ 2 [外部認証 (External Authentication)] をクリックします。
- ステップ 3 [ステータス (Status)] 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 4 [デフォルトユーザ ロール (Default User Role)] ドロップダウンリストから、ユーザ ロールを選択して、外部認証済みユーザに付与するデフォルト権限を定義します。
- ステップ 5 外部サーバを使用して CLI またはシェルアクセスアカウントを認証する場合、[シェル認証 (Shell Authentication)] 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 6 CAC 認証および認可を有効にする場合は、[CAC 認証 (CAC Authentication)] ドロップダウンリストから使用可能な CAC 認証オブジェクトを選択します。CAC 認証および認可の設定の詳細については、[CAC 認証](#)を参照してください。
- ステップ 7 事前設定された認証オブジェクトの使用を有効にするには、オブジェクトの横にあるチェックボックスをオンにします。外部認証を有効にするには、少なくとも 1 つの認証オブジェクトを指定する必要があります。
シェル認証を有効にした場合、CLI またはシェルアクセスを許可するよう設定された認証オブジェクトを選択する必要があります。

同じシステム設定で CLI またはシェルアクセスと、CAC 認証を制御するためには異なる認証オブジェクトを使用します。[CAC 認証およびLDAP シェルアクセスのフィールド](#)を参照してください。
- ステップ 8 必要に応じて、上矢印および下矢印を使用して、認証要求が行われたときに認証サーバがアクセスされる順序を変更できます。
CLI またはシェルアクセスのユーザは、認証オブジェクトがプロファイルの順序で最も高いサーバに対してのみ認証できることに注意してください。
- ステップ 9 [保存 (Save)] をクリックします。

次の作業

- 設定変更を展開します。[設定変更の導入](#)を参照してください。

言語の選択

[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。

別の言語の指定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center 7000 & 8000 シリーズ	任意 (Any)	Admin

この設定は、Firepower Management Center または 7000 および 8000 シリーズ 管理対象デバイスに適用されます。

- Firepower Management Center では、この設定はシステム設定の一部になります。
- 7000 および 8000 シリーズ 管理対象デバイスでは、この設定をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、システム設定変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで、設定は有効にはなりません。



注意

ここで指定した言語は、アプライアンスにログインしたすべてのユーザの Web インターフェイスに使用されます。

手順

- ステップ 1** Firepower Management Center を構成するか従来の管理対象デバイスを構成するかに応じて、次の操作を実行します。
- Management Center : [システム (System)] > [設定 (Configuration)] を選択します。
 - 管理対象デバイス : [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower ポリシーを作成または編集します。
- 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。

次の作業

- 設定変更を展開します。 [設定変更の導入](#) を参照してください。

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。

バナーのテキストにはスペースを使用できますが、タブは使用できません。バナーには複数行のテキストを指定できます。テキストに空の行が含まれている場合、バナーでは、その行が改行 (CR) として表示されます。使用できるのは、改行 (Enter キーを押す) を含む ASCII 文字だけです。改行は2文字としてカウントされます。

Telnet または SSH を介してセキュリティアプライアンスにアクセスしたときに、バナーメッセージを処理するのに十分なシステムメモリがなかった場合や、バナーメッセージの表示を試行して TCP 書き込みエラーが発生した場合には、セッションが閉じます。

カスタム ログインバナーの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center 従来型 (Classic)	任意 (Any)	Admin

SSH または Web インターフェイスからログインするユーザに向けて表示するカスタム ログインバナーを作成できます。

この設定は、Firepower Management Center または従来型の管理対象デバイス (7000 および 8000 シリーズ、ASA FirePOWER および NGIPSv) に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、システム設定変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで、設定は有効にはなりません。

手順

ステップ 1 Firepower Management Center または Classic 管理対象デバイスのいずれを設定しているかに応じて、以下を実行します。

- Management Center : [システム (System)] > [設定 (Configuration)] を選択します。

- 管理対象デバイスの場合 : [デバイス (Devices)]>[プラットフォーム設定 (Platform Settings)] を選択するか、ファイアウォール ポリシーを作成、または編集します。

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。

次の作業

- 設定変更を展開します。 [設定変更の導入](#) を参照してください。

セッションタイムアウト

Firepower システムの Web インターフェイスまたは補助コマンドライン インターフェイスの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分単位で設定できます。シェル (コマンドライン) セッションでも同様のタイムアウトを設定できます。

長期にわたり Web インターフェイスをパッシブかつセキュアにモニタする予定のユーザが、導入内に存在する可能性があります。ユーザ設定オプションで Web インターフェイスのセッションタイムアウトからユーザを除外することができます。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

スマートライセン ス	従来のライセンス	サポートされるデ バイス	サポートされるド メイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center 従来型 (Classic)	任意 (Any)	Admin

この構成は、Firepower Management Center または従来の管理対象デバイス (7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv) に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、構成は、システム構成変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで有効になりません。

システムへのシェルアクセスを制限する必要がある場合、追加オプションによって補助コマンドラインインターフェイスの `expert` コマンドを永続的に無効にすることができます。アプライアンスでエキスパートモードを無効にすると、構成シェルアクセスを持つユーザでも、シェルのエキスパートモードに入ることができなくなります。ユーザが補助コマンドラインインターフェイスのエキスパートモードに入ると、ユーザはシェルに応じた任意の Linux コマンドを実行できます。エキスパートモードに入っていない場合は、コマンドラインユーザはコマンドラインインターフェイスが提供するコマンドだけを実行できます。

手順

-
- ステップ 1** Firepower Management Center を構成するか従来の管理対象デバイスを構成するかに応じて、次の操作を実行します。
- Management Center : [システム (System)] > [設定 (Configuration)] を選択します。
 - 管理対象デバイス : [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower ポリシーを作成または編集します。
- ステップ 2** [シェルタイムアウト (Shell Timeout)] をクリックします。
- ステップ 3** 次の選択肢があります。
- Web インターフェイスのセッションタイムアウトを設定するには、[ブラウザセッションタイムアウト (分) (Browser Session Timeout (Minutes))] フィールドに数値 (分数) を入力します。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を除外する方法については、[ユーザアカウントログインオプション](#)を参照してください。
 - コマンドラインインターフェイスのセッションタイムアウトを設定するには、[シェルタイムアウト (分) (Shell Timeout (Minutes))] フィールドに数値 (分数) を入力します。デフォルト値は 0 で、最大値は 1440 (24 時間) です。
 - 補助コマンドラインインターフェイスで `expert` コマンドを永続的に無効にするには、[`expert` コマンドを永続的に無効化 (Permanently Disable Expert Access)] チェックボックスを選択します。
- 注意** エキスパートモードが無効になった状態でポリシーをアプライアンスに展開した場合、Web インターフェイスまたは補助コマンドラインインターフェイスを介してエキスパートモードにアクセスする機能を復元することはできません。エキスパートモード機能を復元するには、サポートに問い合わせる必要があります。
- ステップ 4** [保存 (Save)] をクリックします。
-

次の作業

- 設定変更を展開します。設定変更の導入を参照してください。

SNMP ポーリング

Firepower Management Center およびクラシック管理対象デバイスには、Simple Network Management Protocol (SNMP) ポーリングを有効にすることができます。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。

この機能を使用して、次の要素にアクセスできます。

- 標準 Management Information Base (MIB)。これには、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。
- 7000 および 8000 シリーズ 管理対象デバイスの追加の MIB。これには、物理インターフェイス、論理インターフェイス、仮想インターフェイス、ARP、NDP、仮想ブリッジ、仮想ルータを通して渡されるトラフィックの統計が含まれます。



(注)

SNMP プロトコルの SNMP バージョンを選択する際は、SNMPv2 では読み取り専用コミュニティのみをサポートし、SNMPv3 では読み取り専用ユーザのみをサポートすることに注意してください。SNMPv3 は AES128 による暗号化もサポートします。

SNMP 機能を有効にすると、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ることに注意してください。

SNMP ポーリングの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center 従来型 (Classic)	任意 (Any)	Admin

この構成は、Firepower Management Center または従来の管理対象デバイス (7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv) に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、構成は、システム構成変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで有効になりません。



- (注) システムをポーリングするには、使用する任意のコンピュータで SNMP アクセスを追加する必要があります。SNMP MIB には展開の攻撃に使用される可能性がある情報も含まれているので注意してください。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お勧めします。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お勧めします。
- SNMPv3 は、読み取り専用ユーザと AES128 による暗号化のみをサポートしています。

はじめる前に

- [システムのアクセスリストの設定](#)の説明に従って、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。

手順

- ステップ 1** Firepower Management Center を構成するか従来の管理対象デバイスを構成するかに応じて、次の操作を実行します。
- Management Center : [システム (System)] > [設定 (Configuration)] を選択します。
 - 管理対象デバイス : [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower ポリシーを作成または編集します。
- 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。
- ステップ 4** 次の選択肢があります。
- [バージョン 1 (Version 1)] または [バージョン 2 (Version 2)] を選択した場合は、[コミュニティストリング (Community String)] フィールドに SNMP コミュニティ名を入力します。手順 13 に進みます。
(注) SNMPv2 は、読み取り専用コミュニティのみをサポートしています。
 - [バージョン 3 (Version 3)] を選択した場合、[ユーザを追加 (Add User)] をクリックするとユーザ定義ページが表示されます。

(注) SNMPv3 は、読み取り専用ユーザと AES128 による暗号化のみをサポートしていません。

- ステップ 5 ユーザ名を入力します。
- ステップ 6 [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 7 [認証パスワード (Authentication Password)] フィールドに SNMP サーバの認証に必要なパスワードを入力します。
- ステップ 8 [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 9 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 10 [プライバシー パスワード (Privacy Password)] フィールドに SNMP サーバに必要な SNMP プライバシー キーを入力します。
- ステップ 11 [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 12 [追加 (Add)] をクリックします。
- ステップ 13 [保存 (Save)] をクリックします。

次の作業

- 設定変更を展開します。 [設定変更の導入](#) を参照してください。

STIG コンプライアンス

米国連邦政府内の組織は、Security Technical Implementation Guides (STIG) に示されている一連のセキュリティチェックリストに準拠しなければならない場合があります。Firepower システムは、米国国防総省で規定している STIG 要件のコンプライアンスをサポートしています。

展開内の任意のアプライアンスで STIG コンプライアンスを有効にする場合は、それをすべてのアプライアンスで有効にする必要があります。非準拠の管理対象デバイスを STIG 準拠の Firepower Management Center に登録したり、STIG 準拠デバイスを非準拠の Firepower Management Center に登録したりすることはできません。

STIG コンプライアンスを有効にした場合、適用可能なすべての STIG に厳格なコンプライアンスが保証されるわけではありません。。

STIG コンプライアンスを有効にすると、ローカル シェル アクセス アカウントのパスワードの複雑さや維持に関するルールが変わります。さらに、STIG コンプライアンス モードでは、SSH のリモートストレージを使用できません。

**注意**

サポートからの支援なしでこの設定を無効にすることはできません。また、この設定はシステムのパフォーマンスに大きく影響する可能性があります。シスコでは、米国国防総省（DoD）のセキュリティ要件に準拠する以外の目的で、STIG コンプライアンスを有効にすることを推奨しません。

STIG コンプライアンスの有効化

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center 従来型 (Classic)	任意 (Any)	Admin

この構成は、Firepower Management Center または従来の管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv）に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、構成は、システム構成変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで有効になりません。

**注意**

展開内の任意のアプライアンスで STIG コンプライアンスを有効にする場合は、それをすべてのアプライアンスで有効にする必要があります。サポートからの支援なしでこの設定を無効にすることはできません。また、この設定はシステムのパフォーマンスに大きく影響する可能性があります。シスコでは、米国国防総省（DoD）のセキュリティ要件に準拠する以外の目的で、STIG コンプライアンスを有効にすることを推奨しません。

手順

- ステップ 1** Firepower Management Center を構成するか従来の管理対象デバイスを構成するかに応じて、次の操作を実行します。
- Management Center : [システム (System)] > [設定 (Configuration)] を選択します。
 - 管理対象デバイス : [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower ポリシーを作成または編集します。
- ステップ 2** [STIG Compliance] をクリックします。

(注) STIG コンプライアンスを有効にすると、アプライアンスがリブートします。Firepower Management Center は、システム設定を保存するとリブートし、管理対象デバイスは、設定の変更を展開するとリブートします。

ステップ 3 STIG コンプライアンスをアプライアンスで永続的に有効にする場合は、[STIG コンプライアンスを有効化 (Enable STIG Compliance)] を選択します。

ステップ 4 [保存 (Save)] をクリックします。

次の作業

- 設定変更を展開します。[設定変更の導入](#)を参照してください。
- アプライアンスがバージョン 5.2.0 より前のバージョンから更新された場合は、STIG コンプライアンスを有効にすると、アプライアンス証明書が再生成されます。展開全体で STIG コンプライアンスを有効にした後、管理対象デバイスを Firepower Management Center に再登録します。

時刻および時刻同期

[時刻 (Time)] ページを使用して、Firepower Management Center、あるいは 7000 または 8000 シリーズデバイスのローカル Web インターフェイスから現在の時刻と時刻源を表示することができます。

時刻の設定は、アプライアンスの大半のページで、[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 [アメリカ/ニューヨーク (America/New York)]) を使用してローカル時間で表示されますが、アプライアンス自体には UTC 時間を使用して保存されます。また、現在の時刻は [時刻の同期 (Time Synchronization)] ページの上部に UTC で表示されます (ローカル時間は [手動 (Manual)] の時計設定オプションで表示されます (有効になっている場合))。

時刻の同期は、[時刻の同期 (Time Synchronization)] ページを使用して管理できます。時刻を同期する場合、以下の方法を選択できます。

- 手動で
- 1 つ以上の NTP サーバを使用 (推奨)

ハードウェアの Firepower Management Center を NTP サーバとして使用できますが、仮想 Firepower Management Center は NTP サーバとして使用しないでください。

リモートの NTP サーバを指定する場合、アプライアンスにそのサーバに対するネットワークアクセス権限が必要です。信頼できない NTP サーバを指定しないでください。NTP サーバへの接続では、構成されたプロキシ設定は使用されません。



(注) 時刻の同期後に、Firepower Management Center と管理対象デバイスの時刻が一致するようにしてください。時刻が一致していない場合、管理対象デバイスが Firepower Management Center と通信する際に意図しない結果が生じるおそれがあります。

時刻の同期

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	Management Center 従来型 (Classic)	任意 (Any)	Admin

この構成は、Firepower Management Center または従来の管理対象デバイス（7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv）に適用されます。

- Firepower Management Center では、この構成はシステム構成の一部です。
- 従来の管理対象デバイスでは、この構成をプラットフォーム設定ポリシーの一部として Firepower Management Center から適用します。

いずれの場合も、システム設定変更を保存するか、共有プラットフォーム設定ポリシーを展開するまで、設定は有効にはなりません。

手順

ステップ 1 Firepower Management Center または Classic 管理対象デバイスのいずれを設定しているかに応じて、以下を実行します。

- Management Center : [システム (System)] > [設定 (Configuration)] を選択します。
- 管理対象デバイス : [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [時間同期 (Time Synchronization)] をクリックします。

ステップ 3 管理対象デバイスで時刻を同期する方法を指定する次のオプションがあります。

- NTP を介して Management Center から時刻を受信するには、[NTP 経由で管理センターから (Via NTP from Management Center)] を選択します。詳細については、[Firepower Management Center からの時間の提供](#)を参照してください。

- [NTP 経由 (Via NTP from)] を選択して、さまざまなサーバから NTP 経由で時刻を受信します。テキストボックスで、NTP サーバの IP アドレスのカンマ区切りリストを入力するか、DNS が有効になっている場合は、完全修飾ホスト名およびドメイン名を入力します。

ステップ 4 [保存 (Save)] をクリックします。

- (注) 設定された NTP サーバと管理対象デバイスを同期するには、数分かかる場合があります。さらに、管理対象デバイスを NTP サーバとして設定されている Management Center と同期する場合、Management Center 自体が NTP サーバを使用するように設定されていると、時刻を同期するのにいくらか時間がかかることがあります。これは、管理対象デバイスに時刻を提供するために、Management Center は設定された NTP サーバとまず同期する必要があるためです。
-

次の作業

- 設定変更を展開します。[設定変更の導入](#)を参照してください。
- Management Center と管理対象デバイスの時刻が一致していることを確認します。