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

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
- syslog への監査ログ メッセージの送信
- HTTP サーバへの監査ログ メッセージの送信
- 外部認証の有効化 （15 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
- syslog への監査ログ メッセージの送信
- 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。

次のタスク

- 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。

次のタスク

- 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。

TLS 証明書を使用して TLS と相互認証を有効にすることで、監査ログ ストリーミング用のチャネルの安全性を確保できます。詳細についてはカスタム監査ログ クライアント証明書を参照してください。

注意 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。

監査ログ メッセージを Syslog に送信する

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）
該当なし	任意（Any）	Management Center 従来型（Classic）	任意（Any）	Admin

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、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
```

TLS 証明書を使用して TLS および相互認証を有効にすることによって、監査ログ ストリーミングのチャネルを保護できます。詳細については、カスタム監査ログクライアント証明書を参照してください。

始める前に

- syslog サーバが機能しており、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 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（Enabled）] を選択します。

ステップ 4 [ホスト（Host）] フィールドにある syslog サーバの 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（6514）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。

（注） このフィールドに無効な IPv4 アドレス（192.168.1.456 など）を入力した場合でも、システムは警告を表示しません。代わりに、システムは無効なアドレスをホスト名として扱います。

ステップ 5 Syslog アラート ファシリティで説明されているとおりに、[ファシリティ（Facility）] リストからファシリティを選択します。

ステップ 6 syslog 重大度レベルで説明されているとおりに、[重大度（Severity）] リストから重大度を選択します。

ステップ 7 オプションで、[タグ（Tag）] フィールドに、syslog 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、syslog に送信されるすべての監査ログ レコードの先頭に「FROMMC」を付加したい場合に、このフィールドに「FROMMC」と入力します。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

- 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 メッセージを HTTP サーバに送信する

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）
該当なし	任意（Any）	Management Center 従来型（Classic）	任意（Any）	Admin

この機能を有効にすると、アプライアンスは、HTTP サーバ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

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、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
```

このストリームのチャネルは、SSL 証明書を使用して TLS と相互認証を有効にすることで保護できます。詳細については、カスタム監査ログ クライアント証明書を参照してください。

始める前に

- 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 または従来型の管理対象デバイスのどちらを設定しているかに応じて、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 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
- 時刻
- `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。

次のタスク

- 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。

カスタム監査ログ クライアント証明書

HTTP サーバまたは syslog サーバに監査ログをストリーミングする場合、Transport Layer Security（TLS）証明書を使ってアプライアンスとサーバ間のチャネルを保護することができます。これにより、信頼されたサーバにシステム監査ログを安全にストリーミングすると同時に、ローカル アプライアンスの使用領域を節約することができます。

監査ログをアプライアンスから外部サーバに安全にストリーミングするには、2 つの要件があります。

- アプライアンスの署名付きクライアント証明書をインポートします。システム情報と指定した ID 情報に基づいて、証明書要求を生成できます。生成された要求を認証局に送信し

て、クライアント証明書を要求します。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。

- Transport Layer Security（TLS）を使用するサーバとの通信チャネルを設定します。

サーバに署名付き証明書の提供を要求します。その証明書を確認するため、1 つ以上の証明書失効リスト（CRL）をロードするようにアプライアンスを設定します。アプライアンスは、サーバ証明書を CRL に記載されている証明書に照らして比較します。サーバが提供した証明書が失効した証明書として CRL に記載されている場合、そのサーバには監査ログをストリーミングできません。

（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。

次の要件のいずれか1つを満たしていないクライアント証明書をインポートすると、監査ログのストリーミングは失敗となります。

- 証明書の署名が、サーバ証明書の署名と同じ CA による署名でない。
- 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ない。

現在の監査ログ クライアント証明書の表示

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**）
該当なし	任意（Any）	Management Center7000 & 8000 シリーズ NGIPSv	グローバルのみ	Admin

重要 ハイ アベイラビリティ設定のスタンバイ Firepower 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 Firepower Management Center からこのタスクを実行することはできません。

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。

（注） ASA FirePOWER デバイスの監査ログ クライアント証明書を表示するには、**show audit_cert** CLI コマンドを使用します。

手順

ステップ 1 Firepower Management Center または従来型の管理対象デバイスのどちらに向けた監査ログのストリーミングを構成しているかに応じて、次のように操作します。

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

監査ログ クライアント証明書の署名要求の生成

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**）
該当なし	任意（Any）	Management Center7000 & 8000 シリーズ NGIPSv	グローバルのみ	Admin

重要 ハイ アベイラビリティ設定のスタンバイ Firepower 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 Firepower Management Center からこのタスクを実行することはできません。

この手順を使用して証明書要求を生成すると、単一のシステムにのみ対応する証明書を生成できます。セキュリティを確保するために、広く知られており、信頼できる CA によって署名された証明書を使用してください。

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。

（注） ASA FirePOWER デバイスの場合は、キー ペアと証明書を手動で生成します。

手順

ステップ 1 Firepower Management Center または従来型の管理対象デバイスのどちらに向けた監査ログのストリーミングを構成しているかに応じて、次のように操作します。

- 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

- 証明機関に証明書要求を送信します。
- 署名された証明書を受信したら、その証明書を要求したアプライアンスにインポートします。監査ログ クライアント証明書のインポートを参照してください。

監査ログ クライアント証明書のインポート

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）
該当なし	任意（Any）	Management Center7000 & 8000 シリーズ NGIPSv	グローバルのみ	Admin

重要 ハイ アベイラビリティ設定のスタンバイ Firepower 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 Firepower Management Center からこのタスクを実行することはできません。

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（証明書パスとも呼ばれる）を提供します。

監査ログのストリーミングは、次に示す条件のいずれかを満たしていないクライアント証明書をインポートすると失敗します。

- 証明書が、サーバ証明書に署名したものと同じ CA によって署名されていない。
- 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ない。

（注） ASA FirePOWER に監査ログ クライアント証明書をインポートするには、CLI コマンド **configure audit_cert import** を使用します。

始める前に

- 証明書署名要求を生成します。監査ログ クライアントの証明書署名要求の生成を参照してください。
- 証明書を要求する認証局に CSR ファイルをアップロードします。

手順

ステップ 1 Firepower Management Center または従来型の管理対象デバイスのどちらに向けた監査ログのストリーミングを構成しているかに応じて、次のように操作します。

- 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 サーバ証明書の要求

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）
該当なし	任意（Any）	Management Center 従来型	グローバルのみ	Admin

重要 ハイ アベイラビリティ設定のスタンバイ Firepower 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 Firepower 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、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） CRL を選択すると、システムは、同じ CRL を使用して、監査ログ証明書の検証と、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。

注意 有効なクライアント証明書をインポートせずに、相互認証を有効にすると、監査ログのストリーミングが失敗します。

始める前に

- 接続に使用するサーバ証明書に署名したものと同じ CA で署名されたクライアント証明書をインポートします。監査ログ クライアント証明書のインポートを参照してください。
- クライアント証明書チェーンをインポートします（必要な場合）。監査ログ クライアント証明書のインポートを参照してください。

手順

ステップ 1 Firepower Management Center または従来型の管理対象デバイスのどちらに向けた監査ログのストリーミングを構成しているかに応じて、次のように操作します。

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

ステップ 3 [TLS の有効化（Enable TLS）] を選択して、監査ログを外部サーバにストリーミングする際に Transport Layer Security を使用します。

ステップ 4 [相互認証の有効化（Enable Mutual Authentication）] を選択します。

ステップ 5 次の 2 つの対処法があります。

- 1 つ以上の CRL を使用してサーバ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 6 に進みます。
- 検証なしでサーバ証明書を承認する場合は、手順 9 に進みます。

ステップ 6 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 7 [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 8 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 9 [保存（Save）] をクリックします。

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る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と、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と、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

始める前に

- 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。

次のタスク

- 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。

次のタスク

- 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。

次のタスク

- 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。

次のタスク

- 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。

始める前に

- 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す。

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 サーバで必要な 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。

次のタスク

- 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。

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。

次のタスク

- 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。