従来型デバイス用の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）
- 従来型デバイスの監査ログ （4 ページ）
- 監査ログ証明書（従来型デバイス） （8 ページ）
- 外部認証の設定 （15 ページ）
- 言語の選択 （17 ページ）
- ログイン バナー （18 ページ）
- セッション タイムアウト （20 ページ）
- SNMP ポーリング （21 ページ）
- セキュリティ認定準拠の （24 ページ）
- 時刻および時刻の同期（従来型デバイス） （28 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
任意（Any）	任意（Any）	従来型	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
- 監査ログ メッセージを従来型デバイスから Syslog に送信する （5 ページ）
- 監査ログ メッセージを HTTP サーバに送信する
- 監査ログ証明書（従来型デバイス） （8 ページ）
- 従来型デバイスでの外部認証の有効化 （16 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
- 従来型デバイスでの時刻同期 （29 ページ）
- セキュリティ認定コンプライアンスの有効化

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。設定変更の展開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	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。設定変更の展開を参照してください。

従来型デバイスの監査ログ

従来型デバイスは、管理センターユーザのアクティビティを読み取り、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。

- 監査ログは、Web インターフェイスの標準イベント 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。システムの監査を参照してください。

- 監査ログ メッセージを syslog に送信するよう、従来型デバイスを設定することができます。監査ログ メッセージを従来型デバイスから Syslog に送信する （5 ページ）を参照してください。
- 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、従来型デバイスを設定することができます。監査ログ メッセージを従来型デバイスから HTTP サーバに送信する （7 ページ）を参照してください。

監査ログ データを外部 syslog または HTTP サーバにストリーミングすると、ローカル デバイスの容量を節約できます。

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。詳細については、監査ログ証明書（従来型デバイス） （8 ページ）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 メッセージを従来型デバイスから 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
該当なし	任意（Any）	従来型	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
```

メッセージに関連付ける重大度、ファシリティ、およびオプション タグを指定できます。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。

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。
- 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、監査ログ証明書（従来型デバイス）（8 ページ）を参照してください。

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。

ステップ 2 **Firepower** ポリシーを作成または編集します。

ステップ 3 [監査ログ（Audit Log）] をクリックします。

ステップ 4 [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 5 [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 6 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 7 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 8 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 9 [保存（Save）] をクリックします。

次のタスク

- ポリシーがデバイスに割り当てられていることを確認します。プラットフォーム設定ポリシーのターゲット デバイスの設定を参照してください。
- 設定変更を展開します。設定変更の展開を参照してください。

監査ログ メッセージを従来型デバイスから 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
該当なし	任意（Any）	従来型	任意（Any）	Admin

この機能を有効にすると、アプライアンスまたはデバイスは、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

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または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
```

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アプライアンスまたはデバイスからアクセスできることを確認します。
- 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、監査ログ証明書を参照してください。

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。

ステップ 2 **Firepower** ポリシーを作成または編集します。

ステップ 3 [監査ログ（Audit Log）] をクリックします。

ステップ 4 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 5 [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 6 [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 7 [保存（Save）] をクリックします。

次のタスク

- ポリシーがデバイスに割り当てられていることを確認します。プラットフォーム設定ポリシーのターゲット デバイスの設定を参照してください。
- 設定変更を展開します。設定変更の展開を参照してください。

監査ログ証明書（従来型デバイス）

クライアント証明書

クライアント証明書を使用して、管理対象の従来型デバイスと監査ログ サーバの間の通信を保護するには、NGIPS デバイスから監査ログをセキュアにストリームする方法 （9 ページ）を参照してください。

（注） 管理対象デバイスの証明書を操作するために Management Center を使用することはできません。管理対象デバイスの証明書を操作するには、ローカル Web インターフェイスを使用して各デバイスに直接ログインする必要があります。

サーバ証明書（Server Certificate）

必要に応じて、監査ログ サーバに署名付き証明書の提供を要求できます。

（注） サーバに署名付き証明書の提供を要求する場合、クライアント証明書はサーバ証明書と同じ認証局によって署名される必要があります。

サーバ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。監査ログ サーバと Management Center 間にセキュアな接続が必要な場合を参照してください。

（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。

NGIPS デバイスから監査ログをセキュアにストリームする方法

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
該当なし	任意（Any）	7000 および 8000 シリーズ	任意（Any）	Admin

信頼できる 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）証明書を使用してアプライアンスとサーバ間のチャネルを保護できます。

各クライアント証明書は、アプライアンスやデバイスごとに異なります。複数のアプライアンスやデバイスがある場合、各デバイスについて次の手順をすべて実行します。

次の手順を使用して、7000 または 8000 シリーズ デバイスから外部サーバへ監査ログを安全にストリーミングします。

始める前に

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

手順

ステップ 1 次の手順を実行して、署名付きクライアント証明書を入手し、デバイスにインストールします。

a) 従来型デバイスの署名付き監査ログ クライアント証明書の取得 （10 ページ）：

システム情報と指定した ID 情報に基づいて、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。

デバイスと監査ログ サーバ間の相互認証が必要な場合、接続に使用するサーバ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、その証明書をデバイスにインポートします。従来型デバイスへの監査ログ クライアント証明書のインポート （12 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。

監査ログ サーバと 7000 および 8000 シリーズ デバイスとの間にセキュアな接続が必要な場合（13 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。次を参照してください。

- 監査ログ メッセージを従来型デバイスから Syslog に送信する （5 ページ）
- 監査ログ メッセージを従来型デバイスから HTTP サーバに送信する （7 ページ）

従来型デバイスの署名付き監査ログ クライアント証明書の取得

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）	7000 & 8000 シリーズ NGIPSv	グローバルだけ	Admin

（注） ASA FirePOWER デバイスの場合は、そのデバイスでキー ペアと証明書を生成します。

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。

7000 または 8000 シリーズのハードウェア デバイスの証明書を取得する場合は、次の手順を使用します。

始める前に

次の点を考慮してください。

- 証明書をインストールするデバイスまたはアプライアンスで、証明書署名要求（CSR）を生成する必要があります。（たとえば、アプライアンス A でデバイス B の証明書署名要求は生成できません。）各デバイスおよびアプライアンスで固有の証明書署名要求を生成する必要があります。
- 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。

- デバイスと監査ログ サーバ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 デバイスの Web ベースのユーザ インターフェイスにアクセスします。7000 または 8000 シリーズ デバイスの Web インターフェイスへのログインを参照してください。

ステップ 2 **[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 3 [監査ログ証明書（Audit Log Certificate）] をクリックします。

ステップ 4 [新規 CSR の生成（Generate New CSR）] をクリックします。

ステップ 5 [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 6 [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 7 [市区町村（Locality or City）] を入力します。

ステップ 8 [組織（Organization）] の名前を入力します。

ステップ 9 [組織単位（部署名）（Organizational Unit (Department)）] の名前を入力します。

ステップ 10 [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 11 [生成（Generate）] をクリックします。

ステップ 12 テキスト エディタで、新しい空のファイルを開きます。

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 *`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 15 [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、デバイスにインポートします。従来型デバイスへの監査ログ クライアント証明書のインポート （12 ページ）を参照してください。

従来型デバイスへの監査ログ 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
該当なし	任意（Any）	7000 & 8000 シリーズ NGIPSv ASA FirePOWER	グローバルだけ	Admin

始める前に

- 従来型デバイスの署名付き監査ログ クライアント証明書の取得 （10 ページ）.
- 正しいデバイス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。各証明書は、アプライアンスやデバイスごとに異なります。
- 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 ASA FirePOWER デバイスに監査ログ クライアント証明書をインポートするには、次を実行します。

デバイスのコマンドライン インターフェイスにアクセスして、CLI コマンド **configure audit_cert import** を使用します。

ステップ 2 7000 または 8000 シリーズ デバイスに監査ログ クライアント証明書をインポートするには、次の手順を実行します

a) デバイスの Web ベースのユーザ インターフェイスにアクセスします。7000 または 8000 シリーズ デバイスの Web インターフェイスへのログインを参照してください。
b) **[システム（System）] > [設定（Configuration）]**を選択します。
c) [監査ログ証明書（Audit Log Certificate）] をクリックします。
d) [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。
e) 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。
f) 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。
g) 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。

h) [保存（Save）] をクリックします。

監査ログ サーバと 7000 および 8000 シリーズ デバイスとの間にセキュアな接続が必要な場合

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
該当なし	任意（Any）	7000 および 8000 シリーズ	グローバルだけ	Admin

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。

（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。

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（従来型デバイス） （8 ページ）を参照してください。
- NGIPS デバイスから監査ログをセキュアにストリームする方法 （9 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 デバイスの Web ベースのユーザ インターフェイスにアクセスします。7000 または 8000 シリーズ デバイスの Web インターフェイスへのログインを参照してください。

ステップ 2 **[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 3 [監査ログ証明書（Audit Log Certificate）] をクリックします。

ステップ 4 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。

ステップ 5 検証せずにサーバ証明書を受け入れる場合（非推奨）、次を実行します。

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

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 6 監査ログ サーバの証明書を検証するには、[相互認証の有効化（Enable Mutual Authentication）] をオンにします。

ステップ 7 （相互認証を有効にした場合）無効な証明書を自動的に認識するには、次を実行します。

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

（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。

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 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。

次のタスク

（オプション）CRL 更新の頻度を設定する場合は、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。

従来型デバイスでの監査ログ 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
該当なし	任意（Any）	7000 および 8000 シリーズ ASA FirePOWER	グローバルだけ	Admin

ログインしているアプライアンスまたはデバイスの監査ログ クライアント証明書のみ表示できます。

手順

ステップ 1 ASA FirePOWER デバイスの現在の監査ログ クライアント証明書を表示するには、次を実行します。

デバイスのコマンドライン インターフェイスにアクセスして、CLI コマンド **show audit_cert** を使用します。

ステップ 2 7000 または 8000 シリーズ ハードウェア デバイスの現在の監査ログ証明書を表示するには、次を実行します。

a) デバイスの Web ベースのユーザ インターフェイスにアクセスします。7000 または 8000 シリーズ デバイスの Web インターフェイスへのログインを参照してください。

b) **[システム（System）] > [設定（Configuration）]**を選択します。

c) [監査ログ証明書（Audit Log Certificate）] 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化した場合、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

従来型デバイスでの外部認証の有効化

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）	7000 および 8000	任意（Any）	Admin

始める前に

- 外部認証の説明に従って、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 使用する外部認証オブジェクトそれぞれの横にあるチェックボックスをクリックします。複数のオブジェクトを有効にすると、ユーザは指定された順序でサーバと照合されます。サーバの順序を変更する場合は、次の手順を参照してください。

シェル認証を有効にする場合は、[シェルアクセスフィルタ（Shell Access Filter）] を含む外部認証オブジェクトを有効にする必要があります。CLI/シェル アクセスのユーザは、認証オブジェクトがリスト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。

CLI と CAC の両方の認証が必要な場合は、各目的のため個別の認証オブジェクトを使用する必要があります。

ステップ 8 （任意）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。

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。設定変更の展開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
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 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、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。設定変更の展開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
任意（Any）	任意（Any）	Management Center 従来型	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。

いずれの場合でも、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設定は有効になりません。

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。設定変更の展開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	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。設定変更の展開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
任意（Any）	任意（Any）	Management Center 従来型	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。設定変更の展開を参照してください。

セキュリティ認定準拠の

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。Firepower システムでは、以下のセキュリティ認定標準規格へのコンプライアンスをサポートします。

- コモン クライテリア（CC）：国際コモン クライテリア承認アレンジメントによって確立された、セキュリティ製品のプロパティを定義するグローバル標準規格
- Unified Capabilities Approved Products List（UCAPL）：米国国防情報システム局（DISA）によって確立された、セキュリティ要件を満たす製品のリスト

（注） 米国政府は、Unified Capabilities Approved Products List（UCAPL）の名称を Defense Information Network Approved Products List（DODIN APL）に変更しました。このドキュメントおよび Firepower Management Center Web インターフェイスでの UCAPL の参照は、DODIN APL への参照として解釈できます。

- 連邦情報処理標準（FIPS）140：暗号化モジュールの要件に関する規定

セキュリティ認定コンプライアンスは、CC モードまたは UCAPL モードで有効にすることができます。セキュリティ認定コンプライアンスを有効にしても、選択したセキュリティ モードのすべての要件との厳密なコンプライアンスが保証されるわけではありません。強化手順についての詳細は、認定機関から提供されている本製品に関するガイドラインを参照してください。

注意 この設定を有効にした場合、無効にすることはできません。アプライアンスを CC モードまたは UCAPL モードでなくす必要がある場合は、アプライアンスを再イメージ化する必要があります。

セキュリティ認定準拠特性

次の表は、CC または UCAPL モードを有効にしたときの動作の変更を示しています。（ログインアカウントの制約は、Webインターフェイスアクセスではなくコマンドラインまたはシェル アクセスを指します。）

システムの変更	CC モード	UCAPL モード
FIPS コンプライアンスは有効です。	○	○
バックアップまたはレポートについては、リモート ストレージは利用できません。	○	○
追加のシステム監査デーモンが開始されます。	なし	○
システム ブートローダは固定されています。	なし	○
追加のセキュリティがログイン アカウントに適用されます。	なし	○
ログインアカウントセッションの自動ログアウトを実行します。	なし	○
再起動キー シーケンスの Ctrl-Alt-Del を無効にします。	なし	○
最大 10 の同時ログイン セッションを実行します。	なし	○
バージョン 6.2.0.3 またはそれ以降の 6.2.0.x パッチでのみ、eStreamer を使用したイベント データのエクスポートがサポートされています。	○	○
ログイン アカウントの厳密なセーフガードを適用します。 • パスワードは、大文字および小文字を組み合わせて最大 15 の英数字として、1 つ以上の数字を含む必要があります。 • パスワードは、辞書に出現する単語であったり、連続する繰り返し文字を含んでいたりすることができません。 • 3 回連続ログインに失敗した場合、そのユーザはロックアウトされます。この場合は、管理者がパスワードをリセットする必要があります。 • パスワード履歴を保存しています。 • ログインが成功した場合は、失敗したログインの履歴を表示します。	なし	○

セキュリティ認定準拠の推奨事項

セキュリティ認定コンプライアンスの使用が有効のときに、次のベストプラクティスを確認することをお勧めします。

- 展開時にセキュリティ認定準拠を有効にするには、最初に Firepower Management Center で有効にし、次に、管理対象のすべてのデバイスの同じモードで有効にします。

  注意 両方が同じセキュリティ認定準拠モードで動作していない限り、Firepower Management Center は管理対象デバイスからイベントデータを受信しません。

- 高可用性設定で Firepower Management Center を使用すると、双方の設定を行い、同じセキュリティ認定準拠モードを使用します。
- 次の機能を使用するようにシステムを設定できません。
  - 電子メールレポート、アラート、データのプルーニング通知。
  - Nmap Scan、Cisco IOS Null Route、Set Attribute Value、ISE EPS の修復。
  - バックアップまたはレポート用のリモート ストレージ。
  - サードパーティ クライアントのシステム データベースへのアクセス。
  - 電子メール、SNMP トラップ、syslog から送信される外部通知、アラート。
  - アプライアンスとサーバの間のチャネルを保護するために、SSL 証明書を使用せずに、HTTP サーバまたは syslog サーバに送信された監査ログ メッセージ。
- バージョン 6.2.0.3 およびそれ以降の 6.2.0.x パッチの場合のみ、eStreamer を使用してイベント データを外部クライアントにエクスポートするようにシステムを設定できます。
- CC モードを使用して展開中に SSO を有効にできません。
- CC モードを使用して展開中に CAC を有効にできません。
- CC または UCAPL モードを使用した展開では、Firepower REST API 経由で Firepower Management Center および管理対象デバイスへのアクセスを無効にします。
- UCAPL モードを使用して展開中に CAC を有効にします。

（注） FirePOWER システムは、次の CC または UCAPL モードをサポートしていませんスタックまたはハイ アベイラビリティ ペアの従来型デバイス

セキュリティ認定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
該当なし	任意（Any）	Management Center 従来型	任意（Any）	Admin

この構成は、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、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、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は、構成が有効になりません。

注意 この設定を有効にした後は、無効にすることはできません。アプライアンスを CC モードまたは UCAPL モードでなくす必要がある場合は、アプライアンスを再イメージ化する必要があります。

始める前に

- アプライアンスでセキュリティ認定コンプライアンスを有効にする前に、展開に組み込む予定のあるすべてのデバイスを Firepower Management Center に登録することをお勧めします。

手順

ステップ 1 設定するアプライアンスの種類に応じて、次のようにします。

- Management Center：**[システム（System）]** > **[設定（Configuration）]** を選択します。
- 従来型管理対象デバイス：**[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 [UCAPL/CC コンプライアンス（UCAPL/CC Compliance）] をクリックします。

（注） UCAPL または CC 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 アプライアンスのセキュリティ認定コンプライアンスを永続的に有効にするには、2 つの選択肢があります。

- [コモン クライテリア（Common Criteria）] モードでセキュリティ認定コンプライアンスを有効にするには、ドロップダウン リストから [CC] を選択します。
- [Unified 機能承認製品リスト（Unified Capabilities Approved Products List）] モードでセキュリティ認定コンプライアンスを有効にするには、ドロップダウン リストから [UCAPL] 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

- まだ適用していない場合は、制御と防御のライセンスを、展開内のすべての従来型アプライアンスに適用します。
- 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、セキュリティ認定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。展開全体でセキュリティ認定コンプライアンスを同じモードで有効にした後、管理対象デバイスを Firepower Management Center に再登録します。
- 設定変更を展開します。設定変更の展開を参照してください。

時刻および時刻の同期（従来型デバイス）

FirePOWER システムを正常に動作させるには、Firepower 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ことが不可欠です。

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）サーバを使用します。

注意 Firepower 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。

従来型デバイスでの時刻同期

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
該当なし	任意（Any）	7000 および 8000 シリーズ ASA FirePOWER NGIPSv	任意（Any）	Admin

FirePOWER システムを正常に動作させるには、Firepower 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ことが不可欠です。

始める前に

- 組織に複数の NTP サーバがある場合は、[システム（System）] > [設定（Configuration）] ページで、時刻の同期用に設定したデバイスと同じ NTP サーバを使用します。指定した値をコピーします。
- 組織に NTP サーバがない場合は、Firepower Management Center を NTP サーバとして使用するように設定する必要があります。#unique_1288を参照してください。

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。

ステップ 2 **Firepower** ポリシーを作成または編集します。

ステップ 3 [時刻の同期（Time Synchronization）] をクリックします。

ステップ 4 従来型管理対象デバイスでの時刻同期の方法を指定するには、次を実行します。

- Firepower Management Center が NTP サーバとして機能するように設定されている場合は、[Management CenterのNTPを使用（Via NTP from Management Center）] を選択します。
- ネットワーク上の NTP サーバから時刻を受信する場合は、[NTPの接続元（Via NTP from）] を選択します。テキスト ボックスに、[システム（System）] > [時刻同期（Time Synchronization）] で入力したのと同じ IP アドレスまたはホスト名を入力します。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

- ポリシーがデバイスに割り当てられていることを確認します。プラットフォーム設定ポリシーのターゲット デバイスの設定を参照してください。

- Firepower システム内に Firepower Threat Defense デバイスがある場合は、これらのデバイスに時刻同期を設定します。脅威に対する防御のための NTP 時刻同期の設定を参照してください。
- 設定変更を展開します。設定変更の展開を参照してください。

（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。

NGIPS デバイスの現在のシステム時刻、ソース、および NTP サーバ接続ステータスの表示

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
該当なし	任意（Any）	7000 および 8000 シリーズ	グローバルだけ	Admin

次の手順を使用して、7000 および 8000 シリーズ ハードウェア デバイスでシステム時刻情報を確認します。

[ユーザ設定（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。

さらに、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（ローカル時刻は手動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））。

（注） タイムゾーン機能（[ユーザ設定（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。ローカル タイムゾーンを使用するようにアプライアンスのシステム クロックを変更した場合は、正確なローカル時刻が表示されるように、それを変更して UTC 時間に戻す必要があります。

手順

ステップ 1 NGIPS ハードウェア デバイスのローカル Web インターフェイスにログインします。

詳細については、7000 または 8000 シリーズ デバイスの Web インターフェイスへのログインを参照してください。

ステップ 2 **[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 3 [時間（Time）] をクリックします。

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 サーバのステータスを参照してください。

NTP サーバのステータス

システムが NTP から時間を同期する場合、Firepower Management Center の [時間（Time）] ページ（[システム（System）] > [設定（Configuration）] メニューの下）と 7000 および 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 NTP ステータスを表示できます。

表 *1 : NTP* ステータス

カラム	説明
NTP サーバ	構成済みの NTP サーバの IP アドレスと名前。
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 サーバを使用できないことを示します。 • [保留（Pending）] は、NTP サーバが新しいか、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 サーバのステータスが不明であることを示します。

カラム	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。
Last Update	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。