



システムポリシーの管理

システムポリシーを使用すると、ASA FirePOWER モジュールで次の管理を行うことができます。

- 監査ログ設定
- メールリレーホストおよび通知アドレス
- SNMPポーリング設定
- STIGコンプライアンス

- システムポリシーの作成 (1 ページ)
- システムポリシーの編集 (2 ページ)
- システムポリシーの適用 (2 ページ)
- システムポリシーールールの削除 (3 ページ)
- アプライアンスのアクセスリストの設定 (3 ページ)

システムポリシーの作成

ライセンス：任意

システムポリシーを設定する代わりに、別の ASA FirePOWER モジュールからシステムポリシーをエクスポートして、ASA FirePOWER モジュールにインポートすることができます。必要に合わせて、インポートされたポリシーを編集してから、それを適用することができます。詳細については、[設定のインポートおよびエクスポート](#)を参照してください。

システムポリシーを作成する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Local] > [System Policy] の順に選択します。

[System Policy] ページが表示されます。

ステップ 2 ドロップダウンリストから、新しいシステムポリシーのテンプレートとして使用する既存のポリシーを選択します。

ステップ3 新しいポリシーの名前を [ポリシー名 (Policy Name)] フィールドに入力します。

ステップ4 新しいポリシーの説明を [ポリシーの説明 (Policy Description)] フィールドに入力します。

ステップ5 [作成 (Create)] をクリックします。

システムポリシーが保存され、[Edit System Policy] ページが表示されます。

システムポリシーの編集

ライセンス：任意

ASA FirePOWER モジュールに現在適用されているシステムポリシーを編集する場合は、変更を保存後にポリシーを再適用してください。詳細については、「[システムポリシーの適用 \(2 ページ\)](#)」を参照してください。

既存のシステムポリシーを編集する方法：

ステップ1 [Configuration] > [ASA FirePOWER Configuration] > [Local] > [System Policy] の順に選択します。

既存のシステムポリシーのリストを含む、[System Policy] ページが表示されます。

ステップ2 システムポリシーの横にある編集アイコン (✎) をクリックします。

[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。ASA FirePOWER モジュールに適用されているシステムポリシーを編集する場合は、編集が完了したら、更新したポリシーを再適用してください。[システムポリシーの適用 \(2 ページ\)](#) を参照してください。

ステップ3 [Save Policy and Exit] をクリックして変更を保存します。変更が保存され、[System Policy] ページが表示されます。

システムポリシーの適用

ライセンス：任意

ASA FirePOWER モジュールには、システムポリシーを適用できます。システムポリシーがすでに適用されている場合、再適用するまで、ポリシーに加えた変更は有効になりません。

システムポリシーを適用する方法：

ステップ1 [Configuration] > [ASA FirePOWER Configuration] > [Local] > [System Policy] の順に選択します。

[System Policy] ページが表示されます。

ステップ2 システムポリシーの横にある適用アイコン (✔) をクリックします。

ステップ3 [Apply] をクリックします。

[System Policy] ページが表示されます。メッセージはシステムポリシーの適用のステータスを示します。

システムポリシー ルールの削除

ライセンス：任意

システムポリシー ルールは、ルールが使用中でも削除できます。ルールが使用中の場合は、新しいポリシーが適用されるまでそのルールが使用されます。システムポリシーは削除できません。

システムポリシー ルールを削除するには、次の手順を実行します。

ステップ1 [Configuration] > [ASA FirePOWER Configuration] > [Local] > [System Policy] の順に選択します。

[System Policy] ページが表示されます。

ステップ2 システムポリシー ルールの横にある削除アイコン (🗑️) をクリックします。ルールを削除するには、[OK] をクリックします。

[System Policy] ページが表示されます。ポリシーを削除するかどうか確認するポップアップメッセージが表示されます。

アプライアンスのアクセス リストの設定

ライセンス：任意

さまざまなシステムポリシーの設定を行うことができます。アプライアンスのアクセス リストの設定

ライセンス：任意

[Access List] ページを使用して、特定のポートのアプライアンスにコンピュータがアクセスできるかを制御できます。デフォルトでは、Web インターフェイスへのアクセスに使用するポート 443 (Hypertext Transfer Protocol Secure (HTTPS))、コマンドラインへのアクセスに使用するポート 22 (Secure Shell (SSH)) が任意の IP アドレスに対して有効です。ポート 161 を介した SNMP アクセスを追加することもできます。SNMP 情報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ることに注意してください。



注意 デフォルトでは、アプライアンスへのアクセスは制限されません。よりセキュアな環境でアプライアンスを稼働させるために、特定の IP アドレスに対してアプライアンスへのアクセスを追加してから、デフォルトのオプションすべてを削除することを検討してください。



(注) SSH を介した CLI またはシェルへのログイン試行が 3 回連続して失敗すると、SSH 接続は終了します。

アクセスリストは、システムポリシーの一部です。新しいシステムポリシーを作成するか、既存のシステムポリシーを編集することによって、アクセスリストを指定できます。いずれの場合も、システムポリシーを適用するまでアクセスリストは有効になりません。

アクセスリストを設定するには、次の手順を実行します。

アクセス：管理者

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Local] > [System Policy] の順に選択します。

[System Policy] ページが表示されます。

ステップ 2 システムポリシーの横にある編集アイコン (✎) をクリックします。

ステップ 3 必要に応じて、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できます。

設定が削除されます。

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、ポリシーを適用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ために、[Add Rules] をクリックすることもできます。

[Add IP Address] ページが表示されます。

ステップ 5 [IP Address] フィールドでは、追加する IP アドレスに応じて以下の選択肢があります。

- 正確な IP アドレス (192.168.1.101 など)
- CIDR 表記を使用した IP アドレスブロック (192.168.1.1/24 など)
- 任意の IP アドレスを示す any

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 [Add] をクリックします。

[Access List] ページが再度表示され、行った変更が反映されます。

ステップ 8 [Save Policy and Exit] をクリックします。

システムポリシーが更新されます。システムポリシーを適用するまで変更は有効になりません。詳細については、「[システムポリシーの適用 \(2 ページ\)](#)」を参照してください。

監査ログの設定

ライセンス：任意

ASA FirePOWER モジュールが外部ホストに監査ログをストリーミングするように、システムポリシーを設定できます。



(注) 外部ホストが機能していて、監査ログを送信する ASA FirePOWER モジュールからアクセスできることを確認する必要があります。

送信元ホスト名は送信される情報の一部です。ファシリティ、重大度、およびオプションのタグを使用して監査ログストリームをより詳細に識別できます。ASA FirePOWER モジュールは、システムポリシーが適用されるまで監査ログを送信しません。

この機能が有効になっている状態でポリシーが適用され、宛先ホストが監査ログを受け入れるように設定された後で、syslog メッセージが送信されます。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-DC3000: admin@10.1.1.2, **Operations > Monitoring, Page View**

監査ログの設定を行うには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Local] > [System Policy] の順に選択します。

[System Policy] ページが表示されます。

ステップ 2 システムポリシーの横にある編集アイコン (✎) をクリックします。

ステップ 3 [Audit Log Settings] をクリックします。

[Audit Log Settings] ページが表示されます。

ステップ 4 [Send Audit Log to Syslog] ドロップダウンメニューから、[Enabled] を選択します。(デフォルト設定では [Disabled] になっています。)

ステップ 5 [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 6 [Facility] フィールドから `syslog` ファシリティを選択します。

ステップ 7 [Severity] フィールドから重大度を選択します。

ステップ 8 必要に応じて、[Tag (optional)] フィールドで参照タグを挿入します。

ステップ 9 外部 HTTP サーバに定期的な監査ログの更新を送信するには、[Send Audit Log to HTTP Server] ドロップダウンリストから [Enabled] を選択します。デフォルト設定では [Disabled] になっています。

ステップ 10 [URL to Post Audit] フィールドに、監査情報を送信する 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`
- `result`
- `time`
- `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りますので注意してください。

ステップ 11 [Save Policy and Exit] をクリックします。

システムポリシーが更新されます。システムポリシーを適用するまで変更は有効になりません。詳細については、「[システムポリシーの適用 \(2 ページ\)](#)」を参照してください。

メールリレー ホストおよび通知アドレスの設定

ライセンス：任意

次の処理を行う場合、メールホストを設定する必要があります。

- 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
- データ切り捨て通知の電子メール送信

- 侵入イベントアラートについての電子メールの使用

アプライアンスとメールリレーホストとの間の通信に使用する暗号化方式を選択し、メールサーバの認証資格情報を指定できます（必要な場合）。設定を行った後、指定された設定を使用してアプライアンスとメールサーバとの間の接続をテストできます。

メールリレーホストを設定するには、次の手順を実行します。

-
- ステップ 1** [Configuration] > [ASA FirePOWER Configuration] > [Local] > [System Policy] の順に選択します。
[System Policy] ページが表示されます。
- ステップ 2** システムポリシーの横にある編集アイコン (✎) をクリックします。
- ステップ 3** [Email Notification] をクリックします。
[Configure Email Notification] ページが表示されます。
- ステップ 4** [Mail Relay Host] フィールドで、使用するメールサーバのホスト名または IP アドレスを入力します。
(注) 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 5** [Port Number] フィールドに、電子メールサーバで使用するポート番号を入力します。ポートは通常、暗号化を使用しない場合は 25、SSLv3 を使用する場合は 465、TLS を使用する場合は 587 です。
- ステップ 6** 暗号化方式を選択するには、次のオプションがあります。
- Transport Layer Security を使用してアプライアンスとメールサーバとの間の通信を暗号化するには、[Encryption Method] ドロップダウンリストから [TLS] を選択します。
 - セキュアソケットレイヤを使用してアプライアンスとメールサーバとの間の通信を暗号化するには、[Encryption Method] ドロップダウンリストから [SSLv3] を選択します。
 - アプライアンスとメールサーバとの間の非暗号化通信を許可するには、[Encryption Method] ドロップダウンリストから [None] を選択します。
- アプライアンスとメールサーバとの間の暗号化された通信では、証明書の検証は不要であることに注意してください。
- ステップ 7** アプライアンスによって送信されるメッセージの送信元の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、[From Address] フィールドに入力します。
- ステップ 8** 必要に応じて、メールサーバに接続する際にユーザ名とパスワードを指定するために、[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 9** 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 10** [Save Policy and Exit] をクリックします。

システムポリシーが更新されます。システムポリシーを適用するまで変更は有効になりません。詳細については、「[システムポリシーの適用 \(2 ページ\)](#)」を参照してください。

SNMP ポーリングの設定

ライセンス：任意

システムポリシーを使用してアプライアンスの Simple Network Management Protocol (SNMP) 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、および 3 をサポートします。

システムポリシー SNMP 機能を有効にすると、アプライアンスで 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。



(注) アプライアンス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。詳細については、[アプライアンスのアクセスリストの設定 \(3 ページ\)](#) を参照してください。SNMP MIB にはアプライアンスの攻撃に使用される可能性のある情報も含まれることに注意してください。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。

SNMP ポーリングを設定するには、次の手順を実行します。

- ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Local] > [System Policy] の順に選択します。
[System Policy] ページが表示されます。
- ステップ 2 システムポリシーの横にある編集アイコン (✎) をクリックします。
- ステップ 3 アプライアンスをポーリングするために使用するコンピュータごとに SNMP アクセスをまだ追加していない場合は、ここで追加してください。詳細については、[アプライアンスのアクセスリストの設定 \(3 ページ\)](#) を参照してください。
- ステップ 4 [SNMP] をクリックします。
[SNMP] ページが表示されます。
- ステップ 5 [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。
ドロップダウンリストに選択したバージョンが表示されます。
- ステップ 6 次の選択肢があります。
 - [Version 1] または [Version 2] を選択した場合、[Community String] フィールドに SNMP コミュニティ名を入力します。ステップ 15 に進みます。

- [Version 3] を選択した場合、[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。

- ステップ 7** [Username] フィールドにユーザ名を入力します。
- ステップ 8** [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 9** [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 10** [Authentication Password] フィールドのすぐ下にある [Verify Password] フィールドに認証パスワードを再入力します。
- ステップ 11** 使用するプライバシープロトコルを [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 [None] を選択します。
- ステップ 12** [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 13** [Privacy Password] フィールドのすぐ下にある [Verify Password] フィールドにプライバシーパスワードを再入力します。
- ステップ 14** [Add] をクリックします。
- ユーザが追加されます。ステップ 6～13 までを繰り返して、さらにユーザを追加できます。ユーザを削除するには、削除アイコン (🗑️) をクリックします。
- ステップ 15** [Save Policy and Exit] をクリックします。
- システムポリシーが更新されます。システムポリシーを適用するまで変更は有効になりません。詳細については、「[システムポリシーの適用 \(2 ページ\)](#)」を参照してください。

STIG コンプライアンスの有効化

ライセンス：任意

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。STIG コンプライアンスオプションは、米国国防総省によって定められた特定の要件に準拠することを目的とした設定を有効にします。

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 に対する厳格なコンプライアンスは保証されません。

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。

STIG コンプライアンスが有効なシステムポリシーを適用すると、アプライアンスは強制的にリブートされることに注意してください。STIG が有効なシステムポリシーをすでに STIG が有効になっているアプライアンスに適用した場合、アプライアンスはリブートしません。STIG が無効なシステムポリシーを STIG が有効になっているアプライアンスに適用した場合、STIG は引き続き有効であり、アプライアンスはリブートしません。



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 コンプライアンスを有効にするには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Local] > [System Policy] の順に選択します。

[System Policy] ページが表示されます。

ステップ 2 システムポリシーの横にある編集アイコン (✎) をクリックします。

ステップ 3 [STIG Compliance] をクリックします。

[STIG Compliance] ページが表示されます。

ステップ 4 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、[Enable STIG Compliance] を選択します。

注意 STIG コンプライアンスが有効なポリシーを適用した後に、STIG コンプライアンスをアプライアンスで無効にすることはできません。コンプライアンスを無効にする必要がある場合は、サポートに連絡してください。

ステップ 5 [Save Policy and Exit] をクリックします。

システムポリシーが更新されます。システムポリシーを適用するまで変更は有効になりません。詳細については、「[システムポリシーの適用 \(2 ページ\)](#)」を参照してください。

アプライアンスに対して STIG コンプライアンスを有効にするシステムポリシーを適用した場合、アプライアンスがレポートすることに注意してください。STIG が有効なシステムポリシーをすでに STIG が有効になっているアプライアンスに適用した場合は、アプライアンスはレポートしないことに注意してください。