



SSL ポリシーの開始

この章では、単純な SSL ポリシーを作成して適用する方法について説明します。また、編集、更新、比較などの SSL ポリシー管理の基本情報も含まれています。

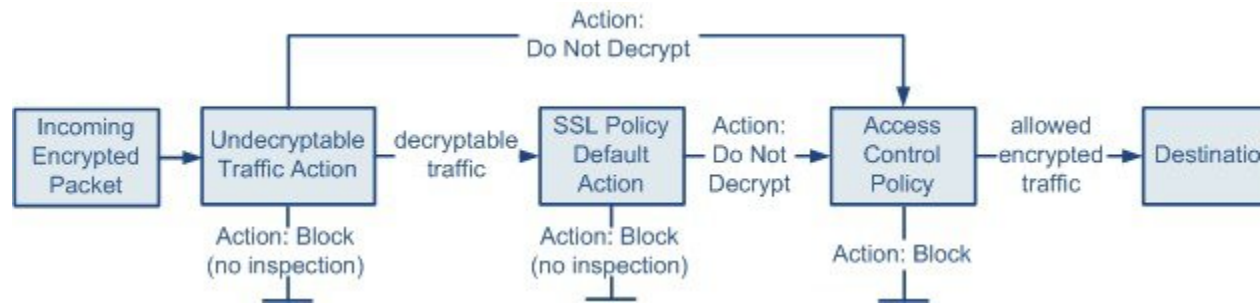
- [SSL ポリシーについて \(1 ページ\)](#)
- [基本 SSL ポリシーの作成 \(2 ページ\)](#)
- [SSL ポリシーの編集 \(8 ページ\)](#)
- [アクセス コントロールを使用した復号化設定の適用 \(10 ページ\)](#)
- [現在のトラフィック復号化設定のレポートの生成 \(11 ページ\)](#)
- [SSL ポリシーの比較 \(13 ページ\)](#)

SSL ポリシーについて

SSL ポリシーは、ネットワーク上の暗号化トラフィックをシステムがどのように処理するかを決定します。SSL ポリシーを、1 つまたは複数設定できます。SSL ポリシーをアクセス コントロール ポリシーに関連付け、そのアクセス コントロール ポリシーを適用します。ASA FirePOWER モジュールで TCP ハンドシェイクが検出されると、アクセス コントロール ポリシーは最初にトラフィックの処理と検査を行います。次に TCP 接続上で SSL 暗号化セッションが識別された場合は、SSL ポリシーが引き継いで、暗号化トラフィックの処理および復号を行います。同時に適用できる SSL ポリシーは 1 つのみです。

最も単純な SSL ポリシーは、次の図のように、単一のデフォルトアクションで暗号化トラフィックを処理するように適用先のデバイスに指示します。デフォルトアクションは、それ以上のインスペクションなしで復号可能なトラフィックをブロックするか、あるいは復号可能なトラフィックを復号化されていない状態でアクセスコントロールによって検査するように設定できます。システムは、暗号化されたトラフィックを許可するか、またはブロックできます。ASA FirePOWER モジュールは復号化できないトラフィックを検出すると、トラフィックをそれ以上検査しないでブロックするか、または復号化しないでアクセスコントロールによる検査

を行います。



より複雑な SSL ポリシーでは、各種の復号化できないトラフィックをさまざまなアクションで処理することが可能であり、認証局（CA）が証明書を発行したか、または暗号化証明書を信頼するかどうかに応じてトラフィックを制御したり、SSL ルールを使ってきめ細かな暗号化トラフィックの制御およびログの記録を行ったりできます。これらのルールには、単純なものや複雑なものがあり、複数の基準を使用して暗号化トラフィックの照合および検査を行います。基本的な SSL ポリシーの作成後は、個々の展開環境に応じた調整法の詳細について、次の章を参照してください。

- [再使用可能オブジェクトの管理](#) では、再利用可能な公開キーインフラストラクチャ（PKI）オブジェクトおよびその他の SSL インспекション関連オブジェクトを設定して、暗号化トラフィックの制御やトラフィックの復号化を強化する方法を説明しています。
- 「[ネットワークトラフィックの接続のロギング](#)」では、復号可能および復号化できない暗号化トラフィックに対するログの設定法を説明しています。
- 「[アクセスコントロールを使用した復号化設定の適用（10 ページ）](#)」では、SSL ポリシーをアクセスコントロールポリシーに関連付ける方法を説明しています。
- 「[アクセスコントロールポリシーの開始](#)」では、アクセスコントロールポリシーをデバイスに適用する方法を説明しています。
- 「[アクセスコントロールルールを使用したトラフィックフローの調整](#)」では、復号化トラフィックを検査するアクセスコントロールルールの設定法を説明しています。
- 「[SSL ルールの開始](#)」では、暗号化トラフィックの処理とログを記録する SSL ルールの設定法を説明しています。
- 「[SSL ルールを使用したトラフィック復号化の調整](#)」では、特定の暗号化トラフィックと SSL ルール条件の一致度を向上させる設定法を説明しています。

基本 SSL ポリシーの作成

ライセンス：任意

新しい SSL ポリシーを作成するために最低限必要な操作は、そのポリシーに一意の名前を付けて、ポリシーのデフォルトアクションを指定することです。新しいポリシーのデフォルトアクションを選択する際には、次のオプションがあります。

- **Do not decrypt** は Do not decrypt デフォルト アクションでポリシーを作成します。
- **Block** は Block デフォルト アクションでポリシーを作成します。
- **Block with reset** は Block with reset デフォルト アクションでポリシーを作成します。

デフォルト アクションは、SSL ポリシーを作成した後で変更できます。デフォルト アクションの選択に関するガイダンスについては、[暗号化トラフィックのデフォルトの処理と検査の設定 \(4 ページ\)](#) を参照してください。

新しい SSL ポリシーにはシステムが復号化できないトラフィックのデフォルト アクションも含まれています。ユーザが復号化できないトラフィックに対して選択したデフォルト アクションを継承する、ブロックする、あるいはトラフィックを復号化せずアクセスコントロールで検査するなどのアクションです。復号化できないトラフィックに対するアクションは、SSL ポリシーの作成後に変更できます。復号できないトラフィックアクションの選択に関するガイダンスについては、[復号できないトラフィックのデフォルト処理の設定 \(5 ページ\)](#) を参照してください。

SSL ポリシーのページ ([Configuration] > [ASA FirePOWER Configuration] > [Policies] > [SSL]) で、オプションの説明とともに、現在のすべての SSL ポリシーを名前別に表示できます。このページのオプションを使用して、さまざまな操作を行うことができます。具体的には、ポリシーの比較、新規ポリシーの作成、ポリシーのコピー、各ポリシーに最近保存された設定をすべてリストするレポートの表示、ポリシーの編集、ポリシーの削除などです。

次の表で、SSL ポリシーのページでポリシーを管理するために実行可能なアクションについて説明します。

表 1: SSL ポリシー管理アクション

目的	操作
新しい SSL ポリシーを作成する	[New Policy] をクリックします。詳細については、「 基本 SSL ポリシーの作成 (2 ページ) 」を参照してください。
既存の SSL ポリシーの設定を変更する	編集アイコン (✎) をクリックします。詳細については、「 SSL ポリシーの編集 (8 ページ) 」を参照してください。
SSL ポリシーを比較する	[Compare Policies] をクリックします。詳細については、「 SSL ポリシーの比較 (13 ページ) 」を参照してください。
SSL ポリシーをコピーする	コピーアイコン (📄) をクリックします。コピーしたポリシーの編集の詳細については、 SSL ポリシーの編集 (8 ページ) を参照してください。
SSL ポリシーの現在の設定を示す PDF レポートを表示する	レポートアイコン (📄) をクリックします。詳細については、「 現在のトラフィック復号化設定のレポートの生成 (11 ページ) 」を参照してください。
SSL ポリシーを削除する	削除アイコン (🗑️) をクリックし、[OK] をクリックします。続行するかどうかを尋ねるプロンプトで、ポリシー内に別のユーザの未保存の変更が存在するかどうかも通知されます。

SSL ポリシーを作成する手順：

- ステップ 1** [Configuration] > > [ASA FirePOWER Configuration] > [Policies] > [SSL] の順に選択します。
[SSL Policy] ページが表示されます。
- ステップ 2** [名前 (Name)] に一意のポリシー名を入力し、オプションで [説明 (Description)] にポリシーの説明を入力します。
スペース、特殊文字、を含めて、印刷可能なすべての文字を使用できます。
- ステップ 3** [Default Action] で、デフォルトアクションを指定します。
選択したデフォルトアクションは、SSL ポリシーの作成後に変更できることに注意してください。詳細については、「[暗号化トラフィックのデフォルトの処理と検査の設定 \(4 ページ\)](#)」を参照してください。
- ステップ 4** [Store ASA FirePOWER Changes] をクリックします。
[SSL Policy Editor] ページが表示されます。詳細については、「[SSL ポリシーの編集 \(8 ページ\)](#)」を参照してください。

暗号化トラフィックのデフォルトの処理と検査の設定

ライセンス：任意

SSL ポリシーのデフォルトアクションは、ポリシーのモニタ以外のルールと一致しない復号可能な暗号化トラフィックについてシステムがどのように処理するかを決定します。SSL ルールがまったく含まれない SSL ポリシーを適用する場合、ネットワーク上のすべての復号可能トラフィックの処理方法を、デフォルトアクションが決定します。システムが復号できない暗号化トラフィックを処理する方法の詳細については、[トラフィック復号の概要](#)を参照してください。

次の表に、選択可能なデフォルトアクションとそれが暗号化トラフィックに対して行う処理をリストします。デフォルトアクションでブロックされた暗号化トラフィックに対しては、システムはいかなる種類のインスペクションも行わないことに注意してください。

:

表 2: SSL ポリシーのデフォルトアクション

デフォルトアクション	暗号化トラフィックに対して行う処理
Block	それ以上のインスペクションは行わずに SSL セッションをブロックする。
Block with reset	それ以上のインスペクションは行わずに SSL セッションをブロックし、TCP 接続をリセットする。
Do not decrypt	アクセス コントロールを使用して暗号化トラフィックを検査する。

SSL ポリシーを最初に作成する場合、デフォルトアクションによって処理される接続のログは、デフォルトでは無効化されています。デフォルトアクションと同様に、この設定もポリシー作成後に変更できます。

次の手順で、ポリシーの編集の際に SSL ポリシーのデフォルトアクションを設定する方法を説明します。SSL ポリシーを編集するための詳細な手順については[SSL ポリシーの編集 \(8 ページ\)](#) を参照してください。

SSL ポリシーのデフォルトアクションを設定する方法：

- ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [SSL] の順に選択します。
[SSL Policy] ページが表示されます。
- ステップ 2 設定する SSL ポリシーの横にある編集アイコンをクリックします。
SSL ポリシー エディタが表示されます。
- ステップ 3 [Default Action] を選択します。詳細については、[暗号化トラフィックのデフォルトの処理と検査の設定 \(4 ページ\)](#) の表を参照してください。
- ステップ 4 [暗号化された接続および復号化できない接続のデフォルトのロギング設定](#)の説明に従って、デフォルトアクションのロギング オプションを設定します。
- ステップ 5 [Store ASA FirePOWER Changes] をクリックします。
[SSL Policy Editor] ページが表示されます。詳細については、「[SSL ポリシーの編集 \(8 ページ\)](#)」を参照してください。

復号できないトラフィックのデフォルト処理の設定

ライセンス：任意

システムによる復号化や検査ができない特定タイプの暗号化トラフィックの処理については、SSL ポリシー レベルで、復号化できないトラフィック用のアクションを設定できます。SSL ルールがまったく含まれない SSL ポリシーを適用する場合、ネットワーク上のすべての復号化できない暗号化トラフィックの処理方法は、復号化できないトラフィック用のアクションが決定します。

復号化できないトラフィックのタイプによって、次の選択ができます。

- 接続をブロックする。
- 接続をブロックした後でリセットする。
- アクセス コントロールを使用して暗号化トラフィックを検査する。
- SSL ポリシーのデフォルトアクションを継承する。

次の表に、復号化できないトラフィックのタイプを示します。

表 3: 復号化できないトラフィック タイプ

タイプ	説明	デフォルト アクション	利用可能なアクション
圧縮されたセッション (Compressed Session)	SSLセッションはデータ圧縮メソッドを適用します。	デフォルト アクションを継承 (Inherit default action)	Do not decrypt Block Block with reset デフォルト アクションを継承 (Inherit default action)
SSLv2 Session	セッションは SSL バージョン 2 で暗号化されます。 トラフィックが復号可能となるのは、クライアントの HELLO メッセージが SSL 2.0 で、送信トラフィックの残りが SSL 3.0 である場合なので注意してください。	デフォルト アクションを継承 (Inherit default action)	Do not decrypt Block Block with reset デフォルト アクションを継承 (Inherit default action)
Unknown Cipher Suite	システムが認識できない暗号スイートです。	デフォルト アクションを継承 (Inherit default action)	Do not decrypt Block Block with reset デフォルト アクションを継承 (Inherit default action)
Unsupported Cipher Suite	検出された暗号スイートに基づく復号化を、システムはサポートしていません。	デフォルト アクションを継承 (Inherit default action)	Do not decrypt Block Block with reset デフォルト アクションを継承 (Inherit default action)
Session not cached	SSLセッションでセッションの再利用が有効化されており、クライアントとサーバがセッション識別子を使ってセッションを再確立しているのに、システムでセッション識別子がキャッシュされていません。	デフォルト アクションを継承 (Inherit default action)	Do not decrypt Block Block with reset デフォルト アクションを継承 (Inherit default action)

タイプ	説明	デフォルト アクション	利用可能なアクション
Handshake Errors	SSLハンドシェイクのネゴシエーション中にエラーが発生しました。	デフォルト アクションを継承 (Inherit default action)	Do not decrypt Block Block with reset デフォルト アクションを継承 (Inherit default action)
Decryption Errors	トラフィックの復号化中にエラーが発生しました。	Block	Block Block with Reset

SSL ポリシーを最初に作成する場合、デフォルト アクションによって処理される接続のログは、デフォルトでは無効化されています。復号化できないトラフィックの処理ではデフォルト アクションのログ設定も適用されるため、復号化できないトラフィック用のアクションで処理される接続のログは、デフォルトでは無効化されています。デフォルトのロギング設定の詳細については、「[SSL ルールを使用した復号可能接続のロギング](#)」を参照してください。



- (注) クライアントとデバイス間に HTTP プロキシがあり、クライアントとサーバが CONNECT HTTP メソッドを使用してトンネル SSL 接続を確立する場合、システムはトラフィックを復号化できません。このトラフィックのシステムによる処理法は、ハンドシェイク エラー (**Handshake Errors**) の復号化できないアクションが決定します。詳細については、「[復号化アクション：さらに検査するためにトラフィックを復号化](#)」を参照してください。

ブラウザが証明書ピンングを使用してサーバ証明書を確認する場合は、サーバ証明書に再署名しても、このトラフィックを復号化できないことに注意してください。このトラフィックはアクセス コントロールを使用して引き続き検査できるため、復号化できないトラフィック アクションでは処理されません。このトラフィックを許可するには、サーバ証明書の共通名または識別名と突き合わせるように、Do not decrypt アクションを使用して SSL ルールを設定します。

復号化できないトラフィックのデフォルト処理を設定する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [SSL] の順に選択します。

[SSL Policy] ページが表示されます。

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

SSL ポリシー エディタが表示されます。

ステップ 3 [Undecryptable Actions] タブを選択します。

[Undecryptable Actions] タブが表示されます。

ステップ 4 各フィールドで、復号化できないトラフィック タイプで実行するアクションを選択するか、あるいは SSL ポリシーのデフォルト アクションを適用するかを指定します。詳細については、[表 2: SSL ポリシーのデフォルト アクション \(4 ページ\)](#) の表を参照してください。

ステップ 5 [Store ASA FirePOWER Changes] をクリックします。

変更を反映させるには、関連付けたアクセスコントロールポリシーを適用する必要があります ([設定変更の導入](#)を参照してください)。

SSL ポリシーの編集

ライセンス：任意

SSL ポリシー エディタでは、ポリシーの設定と SSL ルールの編成ができます。SSL ポリシーの設定では、ポリシーに一意的な名前を付け、デフォルト アクションを指定する必要があります。次のことも実行できます。

- SSL ルールの追加、編集、削除、有効化/無効化
- 信頼できる CA 証明書を追加する
- システムが復号化できない暗号化トラフィックに対する処理の指定
- デフォルト アクションおよび復号化できないトラフィック アクションで処理されるトラフィックのログ

SSL ポリシーの作成または変更後は、SSL ポリシーをアクセスコントロールポリシーに関連付け、そのアクセスコントロールポリシーを適用します。カスタムユーザプロファイルを作成して、ユーザごとに、ポリシーの設定、編成、適用のための異なる権限を割り当てることもできます。

次の表は、SSL ポリシー エディタで実行可能な設定アクションを示しています。

表 4: SSL ポリシーの設定アクション

目的	操作
ポリシーの名前または説明を変更する	[Name] フィールドまたは [Description] フィールドをクリックして、必要に応じて文字を削除し、新しい名前または説明を入力します。
デフォルト アクションを設定する	詳細については、 暗号化トラフィックのデフォルトの処理と検査の設定 (4 ページ) を参照してください。
復号化できないトラフィックのデフォルト処理を設定する	詳細については、 復号できないトラフィックのデフォルト処理の設定 (5 ページ) を参照してください。

目的	操作
デフォルトアクションと復号化できないトラフィックアクションの接続をログに記録する	詳細については、 SSLルールを使用した復号可能接続のロギング を参照してください。
信頼できる CA 証明書を追加する	詳細については、 外部認証局の信頼 を参照してください。
ユーザごとに異なる権限を割り当てる	詳細については、 SSLルールを設定するために必要な情報の収集 を参照してください。
ポリシーの変更を保存する	[保存 (Save)] をクリックします。
ポリシーの変更をキャンセルする	[Cancel] をクリックします。変更を行った場合は、次に [OK] をクリックします。
ポリシーにルールを追加する	[Add Rule] をクリックします。詳細については、「 SSL ルールの概要と作成 」を参照してください。 ヒント ルールの行の空白部分を右クリックし、[Insert new rule] を選択することもできます。
既存のルールを編集する	ルールの横にある編集アイコン (✎) をクリックします。詳細については、 SSL ルールの概要と作成 を参照してください。 ヒント ルールを右クリックして、[Edit] を選択することもできます。
ルールを削除する	ルールの横にある削除アイコン (🗑️) をクリックし、[OK] をクリックします。 ヒント 選択したルールの行の空白部分を右クリックして [Delete] を選択した後、[OK] をクリックして、選択した 1 つ以上のルールを削除するという方法もあります。
既存のルールを有効または無効にする	選択したルールを右クリックして [State] を選択した後、[Disable] または [Enable] を選択します。無効なルールはグレーで表示され、ルール名の下に [(disabled)] というマークが付きます。
特定のルール属性の設定ページを表示する	ルールの行で、該当する条件のカラムに示されている名前、値、またはアイコンをクリックします。たとえば、[Source Networks] カラムに示されている名前または値をクリックすると、選択したルールの [Networks] ページが表示されます。詳細については、「 SSLルールを使用したトラフィック復号化の調整 」を参照してください。

設定を変更すると、変更がまだ保存されていないことを通知するメッセージが表示されます。変更を維持するには、ポリシーエディタを終了する前にポリシーを保存する必要があります。変更を保存しないでポリシーエディタを終了しようとする、変更がまだ保存されていないことを警告するメッセージが表示されます。この場合、変更を破棄してポリシーを終了するか、ポリシーエディタに戻るかを選択できます。

セッションのプライバシーを保護するために、ポリシー エディタで 60 分間操作が行われないと、ポリシーの変更が破棄されて、[SSL Policy] ページに戻されます。30 分間操作が行われなかった時点で、変更が破棄されるまでの分数を示すメッセージが表示されます。以降、このメッセージは定期的に更新されて残りの分数を示します。ページで何らかの操作を行うと、タイマーがキャンセルされます。

複数のユーザが同じポリシーを同時に編集する際、ポリシーエディタに変更を保存していない他のユーザを特定するメッセージが表示されます。いずれかのユーザが変更を保存しようとする、その変更によって他のユーザの変更が上書きされることを警告するメッセージが表示されます。同一のポリシーを複数のユーザが保存する場合、最後に保存された変更が維持されます。

SSL ポリシーを編集する手順：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [SSL] の順に選択します。

[SSL Policy] ページが表示されます。

ステップ 2 次の選択肢があります。

- ポリシーを設定する場合は、[暗号化トラフィックのデフォルトの処理と検査の設定 \(4 ページ\) SSL ルールの開始](#)の表で説明されているすべての操作を使用できます。
- ポリシー ルールを編成する場合は、[SSL ルールの順序指定によるパフォーマンス向上とプリエンブション回避](#)の表で説明されているすべての操作を使用できます。

ステップ 3 設定を保存または廃棄します。次の選択肢があります。

- 変更を保存し、編集を続行する場合は、[Store ASA FirePOWER Changes] をクリックします。
- 変更を廃棄する場合は、[Cancel] をクリックし、プロンプトが出たら [OK] をクリックします。

変更は廃棄され、[SSL Policy] ページが表示されます。

アクセスコントロールを使用した復号化設定の適用

ライセンス：任意

SSL ポリシーに何らかの変更をした後は、関連付けられたアクセス コントロール ポリシーの適用が必要です。詳細については、[設定変更の導入](#)を参照してください。

SSL ポリシーを適用する場合は、次の点に注意してください。

- 適用された SSL ポリシー、または現在適用されている SSL ポリシーを削除することはできません。
- アクセス コントロール ポリシーを適用すると、関連付けられた SSL ポリシーが自動的に適用されます。SSL ポリシーを個別に適用することはできません。



- (注) パッシブ展開では、システムがトラフィックフローに影響を与えることはありません。適用するアクセスコントロールポリシーが参照するSSLポリシーが、暗号化トラフィックをブロックするか、またはサーバ証明書を再署名することでトラフィックを復号化するように設定されている場合、システムから警告が表示されます。また、パッシブ展開では、一時Diffie-Hellman (DHE) および楕円曲線 Diffie-Hellman (ECDHE) 暗号スイートを使用した暗号化トラフィックの復号化をサポートしていません。

SSL ポリシーとアクセスコントロールポリシーを関連付ける方法：

- ステップ 1** [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。
[Access Control Policy] ページが表示されます。
- ステップ 2** 設定するアクセスコントロールポリシーの横にある編集アイコン (✎) をクリックします。
アクセスコントロールポリシー エディタが表示されます。
- ステップ 3** [Advanced] タブを選択します。
アクセスコントロールポリシーの詳細設定が表示されます。
- ステップ 4** [General Settings] の横にある編集アイコン (✎) をクリックします。
[General Settings] ポップアップ ウィンドウが表示されます。
- ステップ 5** [SSL Policy to use for inspecting encrypted connections] ドロップダウンから SSL ポリシーを選択します。
- ステップ 6** [OK] をクリックします。
アクセスコントロールポリシーの詳細設定が表示されます。
- ステップ 7** [Store ASA FirePOWER Changes] をクリックします。
変更を反映させるには、アクセスコントロールポリシーを適用する必要があります ([設定変更の導入](#)を参照してください)。

現在のトラフィック復号化設定のレポートの生成

ライセンス：任意

SSL ポリシー レポートは、特定の時点でのポリシーとルール設定の記録です。このレポートは、監査目的や、現行の設定を調べるために使用できます。



ヒント また、ポリシーを現在適用されているポリシーまたは別のポリシーと比較する **SSL 比較レポート** を生成することもできます。詳細については、[SSL ポリシーの比較 \(13 ページ\)](#) を参照してください。

SSL ポリシー レポートには、次の表で説明するセクションが含まれます。

表 5: SSL ポリシー レポートのセクション

セクション	説明
Title Page	ポリシー レポートの名前、ポリシーが最後に変更された日時、その変更を行ったユーザの名前が記載されます。
Table of Contents	レポートの内容が記載されます。
Policy Information	ポリシーの名前と説明、ポリシーを最後に変更したユーザの名前、ポリシーが最後に変更された日時が記載されます。
Default Action	デフォルト アクションが記載されます。
Default Logging	デフォルト接続ログの設定が記載されます。
Rules	ルール カテゴリ別に、ポリシーに含まれる各ルールのルール アクションおよび条件が記載されます。
Trusted CA Certificates	自動的に信頼できる CA 証明書が記載されます。該当するのは、検出されたトラフィックの暗号化にそうした証明書が使用されている場合、あるいは信頼のチェーン内にある他の証明書が使用されている場合です。
Undecryptable Actions	復号化できないトラフィック タイプが検出された場合に適用されるアクションが記載されます。
Referenced Objects	ポリシーで使用されている個々のすべてのオブジェクトおよびグループ オブジェクトの名前と設定が、各オブジェクトが設定されている条件タイプ別 (ネットワーク、ポート、タグなど) に記載されます。

SSL ポリシー レポートを表示する方法 :

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [SSL] の順に選択します。

[SSL Policy] ページが表示されます。

ステップ 2 レポートの生成対象とするポリシーの横にあるレポートアイコン (📄) をクリックします。SSL ポリシーレポートを生成する前に、すべての変更を保存してください。保存された変更のみがレポートに表示されます。

システムによってレポートが生成されます。ブラウザの設定によっては、レポートがポップアップウィンドウに表示されることがあります。または、コンピュータにレポートを保存するかどうか確認するプロンプトが出される場合があります。

SSL ポリシーの比較

ライセンス：任意

ポリシー変更が組織の標準に準拠しているかどうかを確認するため、またはシステムのパフォーマンスを最適化するために、2つのSSLポリシーの違いを確認することができます。任意の2つのポリシーを比較することも、現在適用されているポリシーを別のポリシーと比較することもできます。オプションで、比較した後にPDFレポートを生成することで、2つのポリシーの間の差異を記録できます。

ポリシーを比較するために使用できるツールは2つあります。

- 比較ビューは、2つのポリシーを左右に並べて表示し、その差異のみを示します。比較ビューの左右のタイトルバーに、それぞれのポリシーの名前が表示されます。ただし、[Running Configuration] を選択した場合、現在アクションなポリシーは空白のバーで表されます。

このツールを使用すると、Web インターフェイスで2つのポリシーを表示してそれらに移動するときに、差異を強調表示することができます。

- 比較レポートは、ポリシーレポートと同様の形式ですが、2つのポリシーの間の差異だけが、PDF形式で記録されます。

これを使用して、ポリシーの比較の保存、コピー、出力、共有を行って、さらに検証することができます。

SSL ポリシー比較ビューの使用

ライセンス：任意

比較ビューには、両方のポリシーが左右に並べて表示されます。それぞれのポリシーは、比較ビューの左右のタイトルバーに示される名前です。現在実行されている設定ではな

い2つのポリシーを比較する場合、最後に変更された日時とその変更を行ったユーザがポリシー名と共に表示されます。2つのポリシー間の違いは次のように強調表示されます。

- 青色は強調表示された設定が2つのポリシーで異なることを示し、差異は赤色で示されます。
- グリーンは、強調表示されている設定項目が一方のポリシーに含まれ、もう一方のポリシーには含まれないことを示します。

次の表に、実行できる操作を記載します。

表 6: SSL ポリシー比較のビューのアクション

目的	操作
変更個別にナビゲートする	またはタイトルバーの上にある [Previous] または [Next] をクリックします。 左側と右側の間にある二重矢印アイコン (⇄) が移動し、[Difference] 番号が調整されて、表示中の差異が示されます。
新しいポリシー比較ビューを生成する	[New Comparison] をクリックします。 [Select Comparison] ウィンドウが表示されます。SSL ポリシー比較レポートの使用を参照してください。
ポリシー比較レポートを生成する	[Comparison Report] をクリックします。 ポリシー比較レポートは、2つのポリシーの間の差異だけをリストした PDF ドキュメントです。

SSL ポリシー比較レポートの使用

ライセンス：任意

SSL ポリシー比較レポートは、ポリシー比較ビューによって示される2つのSSLポリシー間または1つのポリシーと現在適用されているポリシーの間のすべての差異をPDF形式で表示する記録です。このレポートを使用することで、2つのポリシー設定の間の違いをさらに調べ、調査結果を保存して共有できます。

アクセス可能な任意のポリシーに関して、比較ビューからSSLポリシー比較レポートを生成できます。ポリシーレポートを生成する前に、必ずすべての変更を保存してください。レポートには、保存されている変更だけが表示されます。

ポリシー比較レポートの形式は、ポリシーレポートと同様です。唯一異なる点は、ポリシーレポートにはポリシーのすべての設定が記載される一方、ポリシー比較レポートにはポリシー間で異なる設定だけがリストされることです。SSLポリシー比較レポートには、「表 5: SSL ポリシーレポートのセクション (12 ページ)」で説明しているセクションが含まれます。



ヒント 同様の手順を使用して、アクセスコントロールポリシー、ネットワーク解析ポリシー、侵入ポリシー、ファイルポリシー、システムポリシー、またはヘルスポリシーを比較できます。

2つのSSLポリシーを比較する方法：

ステップ1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [SSL] の順に選択します。

[SSL Policy] が表示されます。

ステップ2 [Compare Policies] をクリックします。

[Select Comparison] ウィンドウが表示されます。

ステップ3 [Compare Against] ドロップダウンリストから、比較するタイプを次のように選択します。

- 異なる2つのポリシーを比較するには、[Other Policy] を選択します。

ページが更新されて、[Policy A] と [Policy B] という2つのドロップダウンリストが表示されます。

- 現在アクティブなポリシーと別のポリシーを比較するには、[Running Configuration] を選択します。

ページが更新されて、[Target/Running Configuration A] と [Policy B] という2つのドロップダウンリストが表示されます。

ステップ4 選択した比較タイプに応じて、次のような選択肢があります。

- 2つの異なるポリシーを比較することを選択した場合は、[Policy A] および [Policy B] ドロップダウンリストのそれぞれから、比較するポリシーを選択します。
- 現在実行されている設定を別のポリシーと比較する場合は、[Policy B] ドロップダウンリストから2つ目のポリシーを選択します。

ステップ5 ポリシー比較ビューを表示するには、[OK] をクリックします。

比較ビューが表示されます。

ステップ6 オプションで、[Comparison Report] をクリックして、SSL ポリシー比較レポートを生成します。

SSL ポリシー比較レポートが表示されます。ブラウザの設定によっては、レポートがポップアップウィンドウで表示されるか、コンピュータにレポートを保存するようにプロンプトが出されることがあります。

次のタスク

