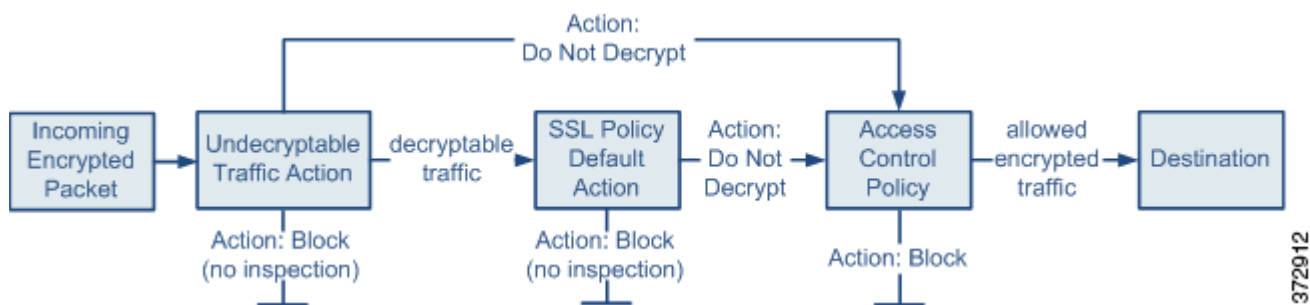




SSL ポリシー クイック スタート ガイド

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します。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化を行います。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のインスペクションなしでブロックするか、あるいは復号化しないままにして、アクセスコントロールによる検査を行います。



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。詳細については、以下を参照してください。

- [基本 SSL ポリシーの作成 \(14-2 ページ\)](#)
- [SSL ポリシーの編集 \(14-7 ページ\)](#)
- [アクセスコントロールを使用した復号化設定の適用 \(14-8 ページ\)](#)
- [現在のトラフィック復号化設定のレポートの生成 \(14-9 ページ\)](#)
- [SSL ポリシーの比較 \(14-10 ページ\)](#)

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\(2-1 ページ\)](#)」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、トラフィックの復号化や暗号化トラフィックの制御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\(35-1 ページ\)](#)」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\(14-8 ページ\)](#)」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\(4-1 ページ\)](#)」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\(6-1 ページ\)](#)」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 ルールクイック スタート ガイド\(15-1 ページ\)](#)」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\(16-1 ページ\)](#)」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:すべて

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\(14-4 ページ\)](#)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。復号化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、[復号化できないトラフィックのデフォルト処理の設定\(14-5 ページ\)](#)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 14-1 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(14-2 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(14-7 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(14-10 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(14-7 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(14-9 ページ) 」を参照してください。
SSLポリシーを削除する	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 [Name]に一意的ポリシー名を入力し、オプションで [Description] にポリシーの説明を入力します。
印刷可能なすべての文字を使用できます。これにはスペースと特殊文字も含まれます。
- 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\(14-4 ページ\)](#)」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\(14-7 ページ\)](#)」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:すべて

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。システムが復号化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、[復号化できないトラフィックのデフォルト処理の設定 \(14-5 ページ\)](#) 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 14-2 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
ブロック	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 \(14-7 ページ\)](#) 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 ポリシーの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、[SSL ポリシーのデフォルト アクション](#)の表を参照してください。
- ステップ 4 「[SSL ルールによる復号可能接続のロギング \(35-15 ページ\)](#)」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 \(14-7 ページ\)](#)」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の設定

ライセンス:すべて

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 14-3 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
Compressed Session	SSLセッションはデータ圧縮メソッドを適用します。	Inherit default action	Do not decrypt ブロック Block with reset 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。	Inherit default action	Do not decrypt ブロック Block with reset 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。	Inherit default action	Do not decrypt ブロック Block with reset 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。	Inherit default action	Do not decrypt ブロック Block with reset 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。	Inherit default action	Do not decrypt ブロック Block with reset Inherit default action

表 14-3 復号化できないトラフィック タイプ(続き)

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。	Inherit default action	Do not decrypt ブロック Block with reset 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。	ブロック	ブロック 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 ルールによる復号可能接続のロギング\(35-15 ページ\)](#)」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\(15-10 ページ\)](#)」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、[SSL ポリシーのデフォルト アクション](#)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 ([設定変更の展開\(4-12 ページ\)](#)を参照してください)。

SSL ポリシーの編集

ライセンス:すべて

SSL ポリシー エディタ ページでは、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、ポリシーに一意の名前を付け、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 14-4 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(14-4 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、 復号化できないトラフィックのデフォルト処理の設定(14-5 ページ) を参照してください。
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 ルールによる復号可能接続のロギング(35-15 ページ) 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(16-22 ページ) 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(13-7 ページ) を参照してください。
ポリシーの変更を保存する	[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(15-4 ページ) 」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]を選択するという方法もあります。
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(15-4 ページ) 」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。

表 14-4 SSL ポリシーの設定アクション(続き)

目的	操作
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(16-1 ページ) 」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、[SSL ポリシーの設定アクション](#)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、[ポリシー内の SSL ルールの管理\(15-13 ページ\)](#)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:すべて

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、[設定変更の展開\(4-12 ページ\)](#)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。適用しようとするアクセス コントロール ポリシーが参照する SSL ポリシーに、暗号化トラフィックのブロックまたは、サーバ証明書の再署名によるトラフィックの復号化が設定されている場合、システムから警告が出されます。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) 暗号スイートを使っ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([設定変更の展開\(4-12 ページ\)](#)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:すべて

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\(14-10 ページ\)](#)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 14-5 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。

SSL ポリシーの比較

ライセンス:すべて

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、現在アクティブ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。

ポリシー比較ツールの概要と使用法の詳細については、次の項を参照してください。

- [SSL ポリシー比較ビューの使用 \(14-11 ページ\)](#)
- [SSL ポリシー比較レポートの使用 \(14-12 ページ\)](#)

SSL ポリシー比較ビューの使用

ライセンス:すべて

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特定されます。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。
- 緑色は強調表示された設定が一方のポリシーには存在するが、他方には存在し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 14-6 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、表示している差異を示す [Difference] 番号が変わります。
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。詳細については、「 SSL ポリシー比較レポートの使用 (14-12 ページ) 」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:すべて

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、「[現在のトラフィック復号化設定のレポートの生成\(14-9 ページ\)](#)」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よって、次の選択肢があります。
 - 2 つの異なるポリシーを比較する場合は、[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。
