



アクセスコントロールポリシーの開始

アクセスコントロールポリシーは、システムがネットワーク上のトラフィックを処理する方法を決定します。各 ASA FirePOWER モジュールには、現在適用されている 1 つのポリシーを設定できます。

この章では、単純なアクセスコントロール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、アクセスコントロールポリシーの管理に関する基本情報（編集、更新、比較など）も含まれています。

- [アクセスコントロールポリシーについて \(1 ページ\)](#)
- [アクセスコントロールのライセンスおよびロール要件 \(3 ページ\)](#)
- [基本的なアクセスコントロールポリシーの作成 \(3 ページ\)](#)
- [アクセスコントロールポリシーの管理 \(7 ページ\)](#)
- [アクセスコントロールポリシーの編集 \(8 ページ\)](#)
- [アクセス制御への他のポリシーの関連付け \(11 ページ\)](#)
- [失効したポリシーの警告について \(12 ページ\)](#)
- [設定変更の導入 \(14 ページ\)](#)
- [アクセスコントロールポリシーとルールのトラブルシューティング \(14 ページ\)](#)
- [現在のアクセスコントロール設定のレポートの生成 \(19 ページ\)](#)
- [アクセスコントロールポリシーを比較する \(20 ページ\)](#)
- [アクセスコントロールポリシーでの詳細設定の使用 \(23 ページ\)](#)

アクセスコントロールポリシーについて

最も単純なアクセスコントロールポリシーは、そのデフォルトアクションを使用してすべてのトラフィックを処理します。このデフォルトアクションは、詳細な検査を行わずにすべてのトラフィックをブロックまたは信頼するように設定することも、侵入についてトラフィックを検査するように設定することもできます。



インライン展開された ASA FirePOWER モジュールだけがトラフィックのフローに影響を与える可能性があることに注意してください。トラフィックをブロックまたは変更するように設定されたアクセスコントロールポリシーをパッシブに展開されたデバイスに適用すると、予期しない結果になることがあります。場合によっては、パッシブに展開された ASA FirePOWER モジュールへのインライン設定の適用がシステムにより阻止されることがあります。

より複雑なアクセスコントロールポリシーはセキュリティインテリジェンスデータに基づいてトラフィックをブロックすることができ、また、アクセス制御ルールを使用してネットワークトラフィックのロギングおよび処理を細かく制御することができます。これらのルールは単純または複雑にすることができ、複数の基準を使用してトラフィックを照合および検査できます。高度なアクセスコントロールポリシーオプションは、復号化、前処理、パフォーマンス、および他の一般設定を制御します。

基本的なアクセスコントロールポリシーを作成した後に、固有の展開環境に合わせて調整する方法については、次の章を参照してください。

- [セキュリティインテリジェンスの IP アドレス レピュテーションを使用したトラフィックのブロック](#) では、最新のレピュテーションインテリジェンスに基づいて接続を直ちにブロックする方法について説明します。
- [ネットワーク分析ポリシーと侵入ポリシーについて](#) では、システムの侵入検知および防止機能の一部として、ネットワーク分析および侵入ポリシーがパケットを前処理し確認する方法について説明します。
- [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、複数の ASA FirePOWER モジュールで、アクセスコントロールルールがネットワークトラフィックを処理する詳細な方法について説明します。
- [侵入ポリシーおよびファイルポリシーを使用したトラフィックの制御](#) では、侵入、禁止されたファイルおよびマルウェアを検出しオプションでブロックすることによって、トラフィックがその宛先に許可される前に、最後の防衛ラインを侵入ポリシーおよびファイルポリシーが提供する方法について説明します。

アクセスコントロールのライセンスおよびロール要件

アクセスコントロールのライセンス要件

アクセスコントロールポリシーは、ASA FirePOWER モジュールのどのライセンスでも作成できますが、アクセスコントロールのある側面では、ポリシーを適用する前に、特定のライセンス機能を有効にする必要があります。

警告アイコンおよび確認ダイアログボックスは、ご使用の展開環境でサポートされない機能を示します。

次の表に、アクセスコントロールポリシーを適用する際のライセンス要件を記載します。

表 1: アクセスコントロールのライセンス要件

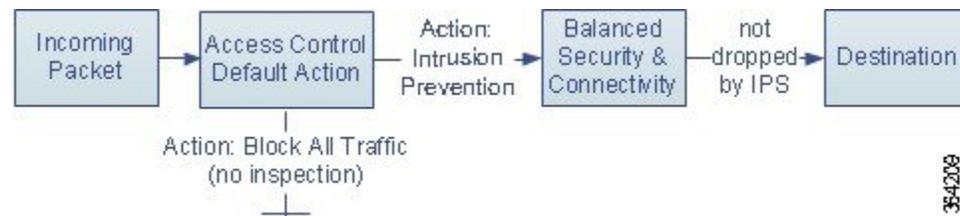
以下を実行するアクセスコントロールポリシーを適用する場合	ライセンス
ゾーン、ネットワーク、またはポートに基づいてアクセスコントロールを実行する リテラル URL および URL オブジェクトを使用して URL フィルタリングを実行する	任意
位置情報データ（発信元または宛先の国/大陸）に基づいてアクセスコントロールを実行する	任意
侵入検知および侵入防御、ファイルコントロール、またはセキュリティインテリジェンス フィルタリングを実行するポリシー	Protection
高度なマルウェア防御としてネットワークベースのマルウェア検出およびブロッキングを実行するポリシー	Malware
ユーザ制御またはアプリケーション制御を実行するポリシー	Control
カテゴリとレピュテーションデータを使用して URL フィルタリングを実行するポリシー	URL Filtering

基本的なアクセスコントロールポリシーの作成

ライセンス：任意

アクセスコントロールポリシーには一意の名前が必須であり、デフォルトアクションを指定する必要があります。この時点で、デフォルトアクションにより、ASA FirePOWER モジュールの暗号化されていないすべてのトラフィックの処理方法が決まります。トラフィックフローに影響するその他の設定は後で追加します。

次の図に示すように、追加のインスペクションなしですべてのトラフィックをブロックするか、または侵入がないかどうかトラフィックを検査するようにデフォルトアクションを設定できます。



ヒント 最初にアクセスコントロールポリシーを作成するときに、デフォルトアクションとしてトラフィックを信頼するように選択することはできません。すべてのトラフィックをデフォルトで信頼する場合は、ポリシーを作成した後にデフォルトアクションを変更します。

新規のアクセスコントロールポリシーを作成したり、既存のアクセスコントロールポリシーを管理したりするには、[Access Control Policy] ページ ([Policies] > [Access Control]) を使用します。

必要に応じて、当初からシステムに付属している Default Trust All Traffic という名前のポリシーを使用および変更できます。

アクセスコントロールポリシーの作成方法：

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。

ヒント この ASA FirePOWER モジュールから既存のポリシーをコピーしたり、別の ASA FirePOWER モジュールからポリシーをインポートしたりできます。ポリシーをコピーするには、コピーアイコンをクリックします。ポリシーをインポートするには、[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。

ステップ 2 [Name] に一意の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。スペースと特殊文字も含まれますが、番号記号 (#)、セミコロン (;)、波カッコ ({}) は使用できません。名前には少なくとも 1 つのスペース以外の文字が含まれている必要があります。

ステップ 3 初期デフォルトアクションを指定します。

- [すべてのトラフィックをブロック (Block All Traffic)] を選択すると、[アクセスコントロール：すべてのトラフィックをブロック (Access Control: Block All Traffic)] をデフォルトアクションとするポリシーが作成されます。
- [侵入防御 (Intrusion Prevention)] を選択すると、[侵入防御：バランスの取れたセキュリティと接続 (Intrusion Prevention: Balanced Security and Connectivity)] をデフォルトアクションとするポリシーが作成されます。

最初のデフォルトアクションを選択する手順、および後でそれを変更する手順については、[デフォルトの処理の設定およびネットワークトラフィックのインスペクション \(5 ページ\)](#) 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。

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。新しいポリシーの設定方法については、[アクセスコントロールポリシーの編集 \(8 ページ\)](#) を参照してください。ポリシーを有効にするには適用する必要があることに注意してください。[設定変更の導入 \(14 ページ\)](#) を参照してください。

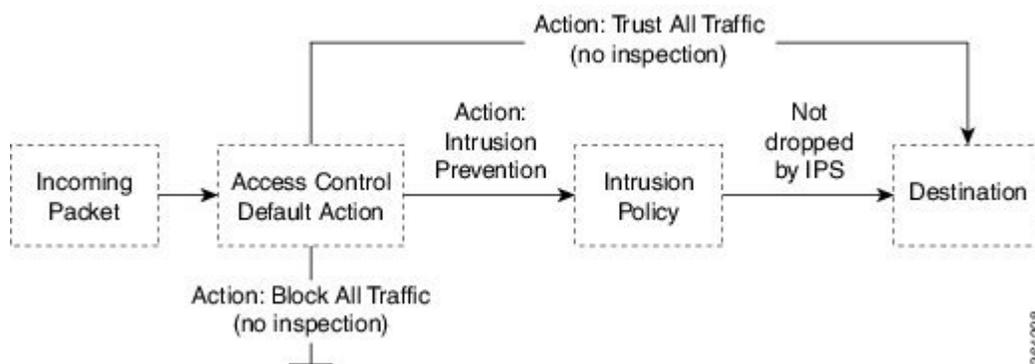
デフォルトの処理の設定およびネットワークトラフィックのインスペクション

ライセンス：任意

アクセスコントロールポリシーを作成する場合は、デフォルトアクションを選択する必要があります。アクセスコントロールポリシーのデフォルトアクションは、次の復号化されたまたは暗号化されていないトラフィックをシステムで処理する方法を決定します。

- セキュリティインテリジェンスによってブロックされない
- ポリシー内のルール of のいずれにも一致しないトラフィック（トラフィックの照合とログインは行うが、処理または検査はしないモナルールを除く）

したがって、アクセスコントロールルールまたはセキュリティインテリジェンスの設定が含まれておらず、暗号化されたトラフィックの処理にSSLポリシーを呼び出さないアクセスコントロールポリシーを適用する場合、デフォルトアクションにより、ネットワーク上のすべてのトラフィックがどのように処理されるかが決まります。追加のインスペクションなしですべてのトラフィックをブロックまたは信頼するか、または侵入がないかトラフィックを検査できます。オプションを次の図に示します。

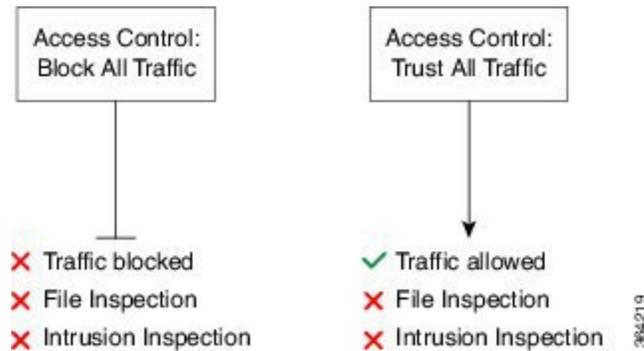


次の表に、さまざまなデフォルトアクションがトラフィックを処理する方法を示し、各デフォルトアクションで処理されるトラフィックで実行できるインスペクションのタイプを示します。デフォルトアクションで処理されるトラフィックでは、ファイルまたはマルウェアのインスペクションを実行できないことに注意してください。詳細については、[侵入ポリシーおよびファイルポリシーを使用したトラフィックの制御](#)を参照してください。

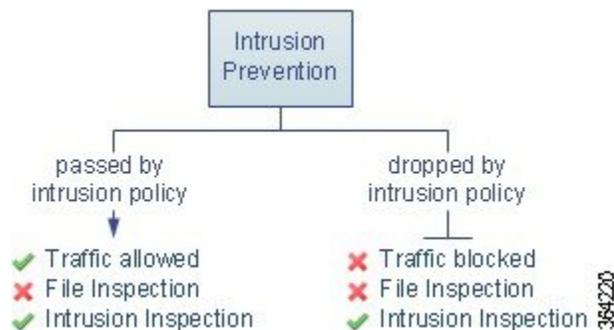
表 2: アクセスコントロールポリシーのデフォルトアクション

デフォルトアクション	トラフィックに対して行う処理	インスペクションのタイプとポリシー
Access Control: Block All Traffic	それ以上のインスペクションは行わずにブロックする	なし
Access Control: Trust All Traffic	信頼 (追加のインスペクションなしで最終宛先に許可)	なし
Intrusion Prevention	ユーザが指定した侵入ポリシーに合格する限り、許可する (Protection ライセンスが必要)	侵入、指定した侵入ポリシーおよび関連する変数セットを使用

次の図は、すべてのトラフィックをブロックおよびすべてのトラフィックを信頼デフォルトアクションを示しています。



以下の図は、侵入防御デフォルトアクションを示しています。



初めてアクセスコントロールポリシーを作成する際、デフォルトアクションで処理される接続のロギングはデフォルトで無効になっています。侵入インスペクションを実行するデフォルトアクションを選択すると、システムはデフォルトの侵入変数セットを選択した侵入ポリシーに自動的に関連付けます。ポリシーを作成した後に、これらのオプションのどちらか、およびデフォルトアクション自体を変更できます。

アクセスコントロールポリシーのデフォルトアクションと関連オプションを変更するには、次の手順を実行します。

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 [Default Action] を選択します。

- すべてのトラフィックをブロックする場合は、[Access Control: Block All Traffic] を選択します
- すべてのトラフィックを信頼する場合は、[Access Control: Trust All Traffic] を選択します
- すべてのトラフィックを侵入ポリシーを使用して検査する場合は、侵入ポリシーを選択します。侵入ポリシーは、いずれも **Intrusion Prevention** というラベルで始まります。侵入ポリシーによってトラフィックがブロックされる可能性があることに注意してください

注意 シスコの担当者から指示された場合を除き、Experimental Policy 1は使用しないでください。シスコでは、試験用にこのポリシーを使用します。

ステップ 4 [Intrusion Prevention] のデフォルトアクションを選択した場合は、変数アイコンをクリックし、選択した侵入ポリシーに関連付けられている変数セットを変更します。

表示されるポップアップ ウィンドウで、新しい変数セットを選択して [OK] をクリックします。編集アイコンをクリックして、選択されている変数セットを新しいウィンドウで編集することもできます。変数セットを変更しない場合、システムはデフォルトのセットを使用します。詳細については、[変数セットの操作](#)を参照してください。

ステップ 5 ロギングアイコンをクリックして、デフォルトアクションによって処理される接続のロギング オプションを変更します。

一致する接続は、その開始時と終了時にログに記録できます。システムはブロックされたトラフィックの終了をロギングできないことに注意してください。ASA FirePOWER モジュール イベント ビューア、外部のシステム ログ (Syslog)、または SNMP トラップ サーバへの接続をログに記録できます。詳細については、[アクセス コントロールの処理に基づく接続のロギング](#)を参照してください。

アクセス コントロール ポリシーの管理

ライセンス : 任意

[Access Control Policy] ページ ([Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control]) で、ポリシーの適用状態に関する情報とともに、現在のカスタム アクセス コントロール ポリシーを確認できます。

ユーザが作成したカスタム ポリシーに加えて、カスタム ポリシー Default Allow All Traffic がシステムによって提供され、それを編集して使用することができます。

[Access Control Policy] ページ上のオプションを使用して、次の表にあるアクションを実行できます。

表 3: アクセスコントロール ポリシーの管理操作

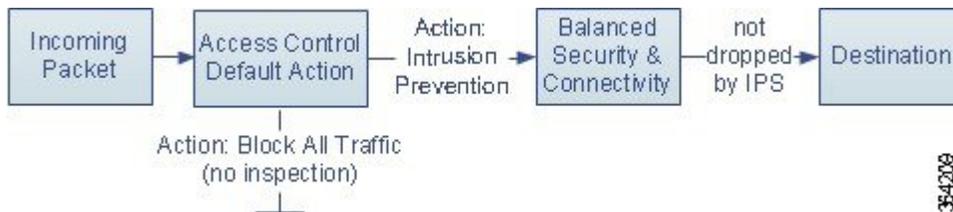
目的	操作	参照先
新しいアクセスコントロールポリシーを作成する	[New Policy] をクリックします。	基本的なアクセスコントロールポリシーの作成 (3 ページ)
既存のアクセスコントロールポリシーを編集する	編集アイコンをクリックします。	アクセスコントロールポリシーの編集 (8 ページ)
アクセスコントロールポリシーを再適用する	適用アイコンをクリックします。	設定変更の導入 (14 ページ)
アクセスコントロールポリシーをエクスポートして別の ASA FirePOWER モジュールにインポートする	エクスポートアイコンをクリックします。	設定のインポートおよびエクスポート
アクセスコントロールポリシーの現行の設定をリストする PDF を表示する	レポートアイコンをクリックします。	現在のアクセスコントロール設定のレポートの生成 (19 ページ)
アクセスコントロールポリシーを比較する	[Compare Policies] をクリックします。	アクセスコントロールポリシーを比較する (20 ページ)
アクセスコントロールポリシーを削除する	削除アイコンをクリックし、ポリシーを削除することを確認します。適用済みのアクセスコントロールポリシーや現在適用しているポリシーは削除できません。	

アクセスコントロールポリシーの編集

ライセンス：任意

新しいアクセスコントロールポリシーを初めて作成する場合、アクセスコントロールポリシー エディタが表示され、[Rules] タブに焦点が置かれています。次の図に、新しく作成されたポリシーを示します。新しいポリシーにはルールやその他の設定がまだ存在しないため、デ

フォルトアクションはすべての暗号化されていないトラフィックを処理します。この場合、デフォルトアクションは、最終宛先に許可する前に、システムによって提供される [バランスの取れたセキュリティと接続 (Balanced Security and Connectivity)] 侵入ポリシーを使用してトラフィックを検査します。



ルールの追加や編成などを行うには、アクセスコントロールポリシーエディタを使用します。次のリストでは、変更可能なポリシー設定に関する情報を提供します。

名前と説明

ポリシーの名前と説明を変更するには、該当するフィールドをクリックし、新しい名前または説明を入力します。

セキュリティ インテリジェンス

セキュリティ インテリジェンスは、悪意のあるインターネット コンテンツに対する最初の防御ラインです。この機能を使用すると、最新のレピュテーションインテリジェンスに基づいて接続を直ちにブロックすることができます。重要なリソースへの継続的なアクセスを確保するために、ブロックリストをカスタムブロックなしリストでオーバーライドできます。このトラフィック フィルタリングは、ルールやデフォルト アクションを含む、他のどのポリシーベースのインスペクション、分析、またはトラフィック処理よりも前に行われます。詳細については、[レピュテーションベースのルールによるトラフィックの制御](#)を参照してください。

ルール

ルールでは、ネットワーク トラフィックを処理する詳細な方法が提供されます。アクセス コントロールポリシー内の各ルールには、1から始まる番号が付きます。システムは、ルール番号の昇順で先頭から順にアクセス コントロールルールをトラフィックと照合します。

ほとんどの場合、システムは、すべてのルールの条件がトラフィックに一致する場合、最初のアクセス コントロールルールに従ってネットワーク トラフィックを処理します。これらの条件には、セキュリティゾーン、ネットワークまたは地理的位置、ポート、アプリケーション、要求されたURL、またはユーザが含まれています。条件は単純または複雑にできます。条件の使用は特定のライセンスによって異なります。

ルールを追加、分類、有効化、無効化、フィルタリング、または管理するには、[Rules] タブを使用します。詳細については、[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](#)を参照してください。

デフォルト アクション

デフォルトアクションは、セキュリティインテリジェンスによってブロックされず、いずれのアクセス制御ルールにも一致しないトラフィックをシステムが処理する方法を決定します。デフォルトアクションを使用して、追加のインスペクションなしですべてのトラフィックをブ

ロックまたは信頼でき、または侵入がないかトラフィックを検査できます。デフォルトアクションによって処理される接続のロギングを有効または無効にできます。

詳細については、[デフォルトの処理の設定およびネットワークトラフィックのインスペクション \(5 ページ\)](#) および[アクセスコントロールの処理に基づく接続のロギング](#)を参照してください。

HTTP 応答

ユーザの Web サイト要求をシステムがブロックした場合にブラウザに表示する内容を指定できます。一般的なシステム提供の応答ページを表示するか、カスタム HTML を入力するかを指定できます。ユーザに警告するページを表示することもできますが、ユーザはボタンをクリックして最初に要求されたサイトをロードするためにページの続行または更新を行うことも可能です。詳細については、[ブロックされた URL のカスタム Web ページの表示](#)を参照してください。

アクセスコントロールの詳細オプション

通常、アクセスコントロールポリシーの詳細設定を変更する必要はほとんど、あるいはまったくありません。デフォルト設定は、ほとんどの展開環境に適しています。変更できる詳細設定には次のものがあります。

- ユーザが要求した各 URL に対し、ASA FirePOWER モジュール データベースに保存する文字数。を参照してください。 [接続で検出された URL のロギング](#)
- ユーザが最初のブロックをバイパスした後に Web サイトを再度ブロックするまでの時間間隔。 [ブロックされた Web サイトのユーザー バイパス タイムアウトの設定](#)を参照してください。
- ネットワーク分析ポリシーおよび侵入ポリシーの設定。この設定では、ネットワークおよびゾーンに対する多くの前処理オプションを調整し、デフォルトの侵入インスペクション動作を設定できます。
- トランスポートおよびネットワーク プリプロセッサの詳細設定。この設定は、アクセスコントロールポリシーを適用するすべてのネットワークおよびゾーンにグローバルに適用されます。
- ユーザのネットワークのホスト オペレーティング システムに基づいて、パッシブ展開でパケットフラグメントおよび TCP ストリームの再構成を改善する適応型プロファイル。 [ルールを使用した侵入ポリシーの調整](#)を参照してください。
- 侵入インスペクション、ファイル制御、および高度なマルウェア防御のパフォーマンスオプション。 [侵入防御パフォーマンスの調整およびファイルおよびマルウェアのインスペクションパフォーマンスおよびストレージの調整](#)を参照してください。

アクセスコントロールポリシーを編集すると、変更がまだ保存されていないことを示す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と、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、[Access Control Policy] ページに戻ります。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。

アクセスコントロールポリシーの編集方法：

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 ポリシーを編集します。上記に要約されているいずれかの操作を実行します。

ステップ 4 設定を保存または廃棄します。

- 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。
- 変更を保存し、ポリシーを適用するには、[Apply ASA FirePOWER Changes] をクリックします。 [設定変更の導入 \(14 ページ\)](#) を参照してください。
- 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。

アクセス制御への他のポリシーの関連付け

ライセンス：任意

次のサブポリシーのいずれかとアクセスコントロールポリシーとを関連付けるには、アクセスコントロールポリシーの詳細設定を使用します。

- SSL ポリシー：セキュアソケットレイヤ (SSL) または Transport Layer Security (TLS) で暗号化されたアプリケーション層プロトコルトラフィックをモニター、復号化、ブロック、または許可します。
- アイデンティティポリシー：トラフィックに関連付けられているレームと認証方式に基づいて、ユーザ認証を実行します。



注意 SSL またはアイデンティティ ポリシーの関連付け、またはそれ以降の [None] を選択することによるポリシー関連付け解除により、設定変更の展開時に Snort プロセスは再開し、トラフィックの検査が一時的に中断されます。この検査中にトラフィックがドロップされるか、それ以上検査が行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。

他の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。

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。

ステップ 3 [Advanced] タブをクリックします。

ステップ 4 適切な [Policy Settings] 領域の編集アイコンをクリックします。

ステップ 5 ドロップダウン リストからポリシーを選択します。

ユーザが作成したポリシーを選択した場合、編集アイコンをクリックして、ポリシーを編集できます。

ステップ 6 [OK] をクリックします。

ステップ 7 設定を保存または廃棄します。

- 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。
- 変更を保存し、ポリシーを適用するには、[Apply ASA FirePOWER Changes] をクリックします。[設定変更の導入 \(14 ページ\)](#) を参照してください。
- 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。

失効したポリシーの警告について

ライセンス：任意

[Access Control Policy] ページ ([Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control]) では、失効したポリシーには、赤色のステータステキストが付いています。

ほとんどの場合、アクセス コントロール ポリシーを変更した場合は、変更を有効にするために再度適用する必要があります。アクセス コントロール ポリシーが他のポリシーを呼び出したり、または他の設定に依存する場合、それらを変更すると、アクセスコントロールポリシーを再度適用する必要があります（または、侵入ポリシーの変更の場合は、侵入ポリシーだけを再度適用できます）。

ポリシーの再適用が必要な設定変更には次のものがあります。

- アクセスコントロールポリシー自体の変更：アクセスコントロールルール、デフォルトアクション、セキュリティインテリジェンスフィルタリング、NAPルールなどの詳細オプションの変更。
- アクセスコントロールポリシーが呼び出す侵入およびファイルポリシーのいずれかの変更：SSLポリシー、ネットワーク分析ポリシー、侵入ポリシー、およびファイルポリシー。
- アクセスコントロールポリシーで使用される再利用可能なオブジェクトまたは設定、またはアクセスコントロールポリシーが呼び出すポリシーの変更：ネットワーク、ポート、URL、および位置情報オブジェクト、セキュリティインテリジェンスのリストとフィード、アプリケーションフィルタまたはディテクタ、侵入ポリシーの変数セット、ファイルリスト、復号化関連オブジェクト、セキュリティゾーンなど。
- システムソフトウェア、侵入ルール、または脆弱性データベース（VDB）の更新。

これらの設定の一部は、ASA FirePOWER モジュールインターフェイスの複数の場所から変更できることに留意してください。たとえば、セキュリティゾーンはオブジェクトマネージャ（[Configuration] > [ASA FirePOWER Configuration] > [Object Management]）を使用して変更できます。

次の更新では、ポリシーの再適用は必要ありません。

- URL フィルタリング データへの自動更新
- スケジュールされた位置情報データベース（GeoDB）の更新

アクセスコントロールポリシーまたは侵入ポリシーが失効した理由を確認するには、比較ビューアを使用します。

アクセスコントロールポリシーが失効した理由を確認するには、次の手順を実行します。

-
- 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。失効したポリシーには、ASA FirePOWER モジュールがポリシーの更新を必要としていることを示す赤色のステータステキストが付いています。
 - ステップ 2** 失効したポリシーのポリシーステータスをクリックします。
詳細な [Apply Access Control Policy] ポップアップウィンドウが表示されます。
 - ステップ 3** 該当する変更されたコンポーネントの横にある [Out-of-date] をクリックします。
ポリシーの比較レポートが新しいウィンドウに表示されます。詳細については、[アクセスコントロールポリシーを比較する（20ページ）](#) および [2つの侵入ポリシーまたはリビジョンの比較](#) を参照してください。
 - ステップ 4** オプションで、ポリシーを再度適用します。「[設定変更の導入（14ページ）](#)」を参照してください。
-

設定変更の導入

ライセンス：任意

ASA FirePOWER モジュールを使用して展開環境の設定を行った後で、その設定に変更を加える場合は、常に新しい設定を展開する必要があります。

この導入アクションにより、次の設定コンポーネントが配布されます。

- アクセスコントロールポリシーとすべての関連ポリシー：DNS、ファイル、アイデンティティ、侵入、ネットワーク分析、SSL
- 導入されたポリシーに関連付けられているすべての関連ルール設定とオブジェクト
- 侵入ルール更新
- デバイスとインターフェイスの設定



注意 特殊なケースとして、設定変更を展開すると、トラフィックフローと処理が一時的に停止したり、いくつかの packets が検査されないまま通過したりすることがあります。利用できない時間を最小限にするために、導入は変更時間帯に実行します。

設定変更を展開するには、次のようにします。

ステップ1 [Deploy] をクリックして、[Deploy FirePOWER Changes] を選択します。

ステップ2 [Deploy] をクリックします。

ステップ3 変更の展開時にエラーまたは警告が出された場合には、次の選択肢があります。

- [Proceed] をクリックして、エラーまたは警告条件を解決しないで導入を続行します。
- [Cancel] をクリックして、展開を実行せずに終了します。エラーおよび警告状態を解決し、設定の再展開を試行します。

アクセスコントロールポリシーとルールのトラブルシューティング

ライセンス：任意

アクセスコントロールポリシーの適切な設定、特に、アクセスコントロールルールの作成と順序付けは複雑なタスクです。しかし、これは効果的な展開を構築するために必要なタスクです。ポリシーを慎重に計画しないと、ルールが他のルールをプリエンブション処理したり、

ルールに無効な設定が含まれる場合があります。ルールおよび他のポリシー設定にはどちらも追加ライセンスが必要な場合があります。

システムが想定どおりにトラフィックを確実に処理できるように、アクセスコントロールポリシーインターフェイスには強力なフィードバックシステムがあります。アクセスコントロールポリシーおよびルールエディタのアイコンは、警告とエラーを示します。表「[アクセスコントロールのエラーアイコン](#)」を参照。



ヒント アクセスコントロールポリシーエディタで、ポリシーのすべての警告を表示するポップアップウィンドウを表示するには [Show Warnings] をクリックします。

また、トラフィックの分析およびフローに影響を与える可能性がある問題の適用時には、システムによって警告が表示されます。

表 4: アクセスコントロールのエラーアイコン

アイコン	説明	詳細
	エラー	ルールまたは設定にエラーがある場合、影響を受けるルールを無効にしても、問題を修正するまでポリシーを適用できません。
	警告	<p>ルールまたはその他の警告を表示するアクセスコントロールポリシーを適用できます。しかし、警告とマークされている誤った設定には影響しません。</p> <p>たとえば、プリエンブション処理されたルールまたは誤った設定（空のオブジェクトグループを使用した条件、アプリケーションに一致しないアプリケーションフィルタ、クラウド通信を有効にしないまま行った URL 条件の設定など）によってトラフィックを照合できないルールを含むポリシーを適用できます。これらのルールは、トラフィックを評価しません。警告が出されているルールを無効にすると、警告アイコンが消えます。潜在する問題を修正せずにルールを有効にすると、警告アイコンが再表示されます。</p> <p>別の例としては、多くの機能で特定のライセンスが必要です。アクセスコントロールポリシーは、対象のデバイスのみ normally 適用されます。</p>
	情報	<p>情報アイコンには、トラフィックのフローに影響する可能性がある設定に関する有用な情報が表示されます。これらの問題によってポリシーの適用が阻まれることはありません。</p> <p>たとえば、アプリケーション制御または URL フィルタリングを実行している場合、システムはその接続でアプリケーションまたは Web トラフィックを識別するまで、接続の最初の数パケットを複数のアクセスコントロールルールと照合するのをスキップする場合があります。これにより、アプリケーションと HTTP 要求が識別されるように接続が確立されます。詳細については、アプリケーション制御の制限およびURL の検出とブロッキングのガイドラインと制限事項を参照してください。</p>

アクセスコントロールポリシーおよびルールを適切に設定することで、ネットワークトラフィックの処理に必要なリソースも減らすことができます。複雑なルールの作成、多数のさま

さまざまな侵入ポリシーの呼び出し、およびルールの誤った順序付けはすべて、パフォーマンスに影響する可能性があります。

パフォーマンスを向上させるためのルールの簡素化

複雑なアクセスコントロールポリシーおよびルールは、重要なリソースを消費する可能性があります。アクセスコントロールポリシーを適用すると、システムはすべてのルールをまとめて評価し、ネットワークトラフィックを評価するためにASA FirePOWERモジュールが使用する条件の拡張セットを作成します。サポートされるアクセスコントロールルールまたは侵入ポリシーの最大数を超過していることを警告するポップアップウィンドウが表示される場合があります。

アクセスコントロールルールの簡素化

次のガイドラインは、アクセスコントロールルールを簡素化し、パフォーマンスを向上させるのに役立ちます。

- ルールを構築するときは、条件内で使用する個々の要素は可能な限り少なくします。たとえばネットワーク条件であれば、個別のIPアドレスではなく、IPアドレスブロックを使用します。ポート条件では、ポート範囲を使用します。アプリケーション制御およびURLフィルタリングを実行する場合はアプリケーションフィルタとURLカテゴリおよびレピュテーションを使用し、ユーザ制御を実行する場合はLDAPユーザグループを使用します。

アクセスコントロールルールの条件で使用する要素をオブジェクトに組み合わせてもパフォーマンスは向上しないことに注意してください。たとえば、50の個別のIPアドレスを含むネットワークオブジェクトを使用しても、その条件内のそれらのIPアドレスに対するものを含む、組織的な（パフォーマンスではない）利点が個別に与えられるだけです。

- できるだけセキュリティゾーンでルールを制限します。デバイスのインターフェイスが、ゾーン制限されたルールのどのゾーンにも属さない場合、そのデバイスのパフォーマンスにルールは影響を与えません。
- ルールを過度に設定しないようにします。1つの条件が処理するトラフィックに一致するのに十分な場合は、2つ使用しないでください。

侵入ポリシーと変数セットの急増の回避

アクセスコントロールポリシーでトラフィックを検査するために使用できる一意の侵入ポリシーの数は、ポリシーの複雑度によって異なります。1つの侵入ポリシーを各許可ルールおよびインタラクティブブロックルール、さらにデフォルトアクションに関連付けることができます。侵入ポリシーと変数セットの固有のペアはすべて、1つのポリシーとしてカウントされます。アクセスコントロールポリシー全体で、侵入ポリシーを3つしか選択できない場合があります。

サポートされる侵入ポリシーの数を超えた場合、アクセスコントロールポリシーを再評価してください。複数の侵入ポリシーまたは変数セットを統合すると、複数のアクセスコントロールルールに1つの侵入ポリシーと変数セットのペアを関連付けることができます。

アクセスコントロールポリシーの次の場所のそれぞれで、選択したポリシーの数と、それらのポリシーが使用する変数セットの数を確認します。アクセスコントロールポリシーの詳細設定の [Intrusion Policy used before Access Control rule is determined] オプション、アクセスコントロールポリシーのデフォルトアクション、およびポリシー内のアクセスコントロールルールのインスペクション設定。

ルールのプリエンプションと無効な設定の警告について

ライセンス：任意

アクセスコントロールルール（および、高度な展開ではネットワーク分析ルール）の適切な設定と順序付けは、効果的な展開を構築するために必須です。アクセスコントロールポリシー内では、アクセスコントロールルールが他のルールをプリエンプション処理したり、ルールに無効な設定が含まれている場合があります。同様に、アクセスコントロールポリシーの詳細設定を使用して設定するネットワーク分析ルールにも同じ問題が存在する可能性があります。システムは、警告とエラーのアイコンを使用してこれらをマークします。

ルールのプリエンプションの警告について

アクセスコントロールルールの条件が後続のルールよりも優先して適用され、後続のルールによるトラフィックの照合が回避される場合があります。次に例を示します。

```
Rule 1: allow Admin users
```

```
Rule 2: block Admin users
```

上記の最初のルールによってトラフィックは事前に許可されているため、2番目のルールによってトラフィックがブロックされることはありません。

次の点に注意してください。

- どのようなタイプのルール条件でも、後続のルールを回避する可能性があります。
- あるルールとその後続のルールがまったく同じで、いずれもすべて同じ条件が設定されている場合、後続のルールは回避されます。
- 条件が1つでも異なる場合は、後続のルールが回避されることはありません。

無効な設定の警告について

アクセスコントロールポリシーが依存する外部の設定は変更される可能性があるため、有効であったアクセスコントロールポリシー設定が無効になる場合があります。次の例について考えてみます。

- ルールの送信元ポートにポートグループを追加し、その後そのポートグループを変更してICMPポートを含めると、そのルールは無効になり、横に警告アイコンが表示されます。ポリシーをまだ適用することはできますが、ルールはネットワークトラフィックに影響を与えません。

- ルールにユーザを追加した後、LDAP ユーザ認識設定を変更してそのユーザを除外すると、ユーザはアクセスコントロールの対象ユーザではなくなるため、そのルールは影響しなくなります。

パフォーマンスを向上させプリエンプションを回避するためのルールの順序付け

ライセンス：任意

アクセスコントロールポリシー内の各ルールには、1から始まる番号が付きます。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。Monitor ルールを除き、トラフィックが最初に一致するルールが、当該トラフィックを処理するためのルールになります。

アクセスコントロールルールの順序を適切にすることで、ネットワークトラフィックの処理に必要なリソースが減り、ルールのプリエンプションを回避できます。ユーザーが作成するルールはすべての組織と展開に固有のもですが、ユーザーのニーズに対処しながらもパフォーマンスを最適化できるルールを順序付けする際に従うべきいくつかの一般的なガイドラインがあります。

ルール条件は高いものから低いものに順序付ける

最初に、組織のニーズに適する順番でルールを配置します。すべてのトラフィックに適用する必要があるプライオリティルールをポリシーの先頭部分付近に配置します。たとえば、ある1人のユーザからのトラフィックに侵入がないかを検査する（許可ルールを使用）が、部門内の他のすべてのユーザは信頼する（信頼ルールを使用）場合は、その順序で2つのアクセスコントロールルールを配置します。

特定のルールから一般的なルールへの順序付け

具体的なルール、つまり処理するトラフィックの定義を絞り込むルールを先に設定することで、パフォーマンスを向上させることができます。これは、広範な条件を持つルールが多くさまざまなタイプのトラフィックを照合し、後でより多くの特定のルールをプリエンプション処理することができるという理由からも重要です。

ほとんどのソーシャルネットワーキングサイトをブロックする一方で、特定の他の部分へのアクセスを許可する場合のシナリオを考えます。たとえば、グラフィックデザイナーに Creative Commons Flickr および deviantART コンテンツへのアクセスを許可したいが、Facebook や Google+ などの他のサイトへのアクセスは許可したくない場合があります。この場合はルールを次のように順序付けする必要があります。

```
Rule 1: Allow Flickr, deviantART for the "Design" LDAP user group
Rule 2: Block social networking
```

ルールを入れ替える場合は次のようになります。

```
Rule 1: Block social networking
Rule 2: Allow Flickr, deviantART for the "Design" LDAP user group
```

最初のルールは、Flickr および deviantART を含むすべてのソーシャル ネットワーキング トラフィックをブロックします。トラフィックが2番目のルールに一致しないため、利用可能にしたかったコンテンツにデザイナーはアクセスできません。

トラフィックを後で検査するルールの配置

侵入、ファイルおよびマルウェアのインスペクションにはリソースの処理が必要なため、トラフィックのインスペクションを行うルール（許可、インタラクティブブロック）の前にトラフィックを検査しないルール（信頼、ブロック）を配置することで、パフォーマンスを向上させることができます。これは、信頼ルールおよびブロックルールは、システムが別の方法で検査をした可能性があるトラフィックを迂回させることができるためです。他の要素がすべて同等、つまり、より重要なものがなくプリエンプションが問題ではない場合にルールのセットを与えると仮定すると、次の順序でルールを配置することを検討します。

- 一致する接続はロギングするが、トラフィックで他のアクションは実行しないモニタールール
- 追加のインスペクションなしでトラフィックを処理する信頼ルールおよびブロックルール
- トラフィックの追加のインスペクションを行わない許可ルールおよびインタラクティブブロックルール
- マルウェア、侵入、またはその両方がないか任意でトラフィックを検査する許可ルールおよびインタラクティブブロックルール

現在のアクセスコントロール設定のレポートの生成

ライセンス：任意

アクセスコントロールポリシーレポートとは、特定の時点でのポリシーおよびルールを設定を記録したものです。このレポートには、次の情報が含まれており、監査目的や現在の設定を調べるために使用できます。

表 5: アクセスコントロールポリシーレポートのセクション

セクション	説明
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。
HTTP Block Response HTTP Interactive Block Response	ポリシーを使用して Web サイトをブロックするときにユーザに表示されるページの詳細が提供されます。
Security Intelligence	ポリシーのセキュリティ インテリジェンスのブロックなしリストとブロックリストの詳細が提供されます。

セクション	説明
Default Action	デフォルトアクションと関連する変数セット（存在する場合）が示されます。
Rules	ポリシーの各アクセスコントロールルールが示され、その設定の詳細が提供されます。
Advanced Settings	次のようなポリシーの詳細設定の情報 <ul style="list-style-type: none"> • アクセスコントロールポリシーのトラフィックを前処理するために使用されるネットワーク分析ポリシー、およびグローバル前処理オプション • パッシブ展開用の適合型プロファイル設定 • ファイル、マルウェア、および侵入を検出するためのパフォーマンス設定 • 他のポリシー全体の設定
Referenced Objects	侵入ポリシーの変数セットおよびSSLポリシーで使用されるオブジェクトなど、アクセスコントロールポリシーによって参照される再利用可能なオブジェクトに関する詳細が提供されます。

また、ポリシーを現在適用されているポリシーや別のポリシーと比較する、アクセスコントロール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、[アクセスコントロールポリシーを比較する（20 ページ）](#)を参照してください。

アクセスコントロールポリシー レポートの表示方法：

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 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。アクセスコントロールポリシー 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、保存された変更のみが表示されます。

システムによってレポートが生成されます。コンピュータにレポートを保存するように求められます。

アクセスコントロールポリシーを比較する

ライセンス：任意

組織の標準に準拠しているかを確認する目的や、システムパフォーマンスを最適化する目的でポリシーの変更を検討するために、2つのアクセスコントロールポリシーの差異を調べること

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示されます。

このツールを使用すると、モジュール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。

アクセスコントロール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せん。
- 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: アクセスコントロールポリシー比較ビューの操作

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。

目的	操作
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、「 アクセスコントロールポリシー比較レポートの使用 (22 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。

アクセスコントロールポリシー比較レポートの使用

ライセンス：任意

アクセスコントロールポリシー比較レポートとは、ポリシー比較ビューで識別された、2つのアクセスコントロールポリシーの間、またはポリシーと現在適用中のポリシーの間にあるすべての差異を、PDF 形式で記録したものです。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。

ユーザは、アクセス権限が与えられている任意のポリシーの比較ビューから、アクセスコントロール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。アクセスコントロールポリシー比較レポートには、「[現在のアクセスコントロール設定のレポートの生成](#)」で説明されているセクションが含まれています。



ヒント 同様の手順を使用して、SSL、ネットワーク分析ポリシー、侵入ポリシー、ファイルポリシー、またはシステムポリシーを比較できます。

2つのアクセスコントロールポリシーを比較する方法：

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 [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場合、[Policy A] ドロップダウン リストと [Policy B] ドロップダウン リスト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 必要に応じて、アクセスコントロールポリシー比較レポートを生成するには [Comparison Report] をクリックします。

アクセスコントロールポリシー比較レポートが表示されます。コンピュータにレポートを保存するように求められます。

アクセスコントロールポリシーでの詳細設定の使用

通常、アクセスコントロールポリシーの詳細設定を変更する必要はほとんど、あるいはまったくありません。デフォルト設定は、ほとんどの展開環境に適しています。アクセスコントロールポリシーでの前処理およびパフォーマンスの詳細オプションの多くは、ルールの更新で変更される場合があることに注意してください。

一般設定

ユーザが要求した各 URL に対し、ASA FirePOWER モジュール データベースに保存する文字数をカスタマイズするには、[接続で検出された URL のロギング](#)を参照してください。

ユーザが最初のブロックをバイパスした後に Web サイトを再度ブロックするまでの時間間隔をカスタマイズするには、[ユーザが URL ブロックをバイパスすることを許可する](#)を参照してください。

ネットワーク分析ポリシーと侵入ポリシー

ネットワーク分析ポリシーおよび侵入ポリシーの詳細設定によって、以下が可能になります。

- システムがトラフィックを検査する方法を正確に決定する前に、最初にそのトラフィックを検査するために使用される、アクセスコントロールポリシーのデフォルトの侵入ポリシーと関連付けられている変数セットの変更。

- 多くの前処理オプションを制御する、アクセスコントロール ポリシーのデフォルト ネットワーク分析ポリシーの変更。
- カスタムネットワーク分析ルールおよびネットワーク分析ポリシーを使用した、特定のセキュリティゾーンおよびネットワークに対する前処理オプションの調整。

ファイルおよびマルウェアの設定

ファイルおよびマルウェアの詳細設定では、ファイル制御および高度なマルウェア防御のためのパフォーマンスオプションを設定できます。詳細については、[許可されたトラフィックに対する侵入およびマルウェアの有無のインスペクション](#)を参照してください。

トランスポート層とネットワーク層のプリプロセッサの設定

トランスポートおよびネットワークのプリプロセッサの詳細設定は、アクセスコントロールポリシーを適用するすべてのネットワーク、ゾーン、およびVLANにグローバルに適用されます。高度なプリプロセッサの詳細については、お使いのバージョンの *Firepower Management Center* コンフィギュレーションガイドの「Advanced Network Analysis and Preprocessing」を参照してください。

パフォーマンス設定および遅延ベースのパフォーマンス設定

[パケットおよび侵入ルール遅延しきい値の設定](#)では、侵入行為についてトラフィックを分析する際のシステムのパフォーマンスを向上させるための情報を提供しています。