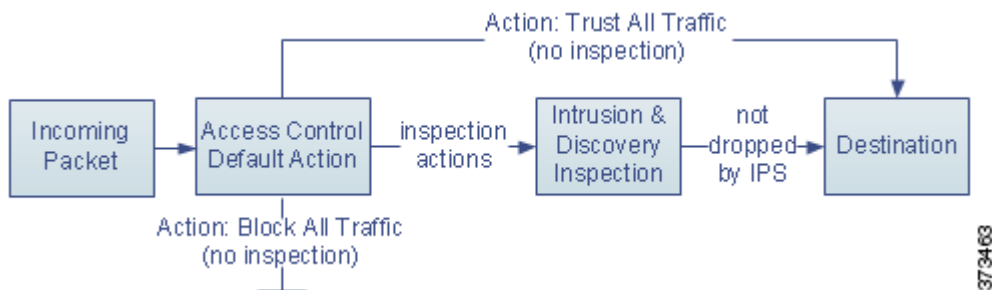




アクセスコントロールポリシーの準備

アクセスコントロールポリシーは、ネットワーク上の非高速パスを通るトラフィックを、システムでどのように処理するかを決定します。1つ以上のアクセスコントロールポリシーを設定して、設定したポリシーを1つ以上の管理対象デバイスに適用できます。各デバイスに同時に適用できるポリシーは1つです。

最も単純なアクセスコントロールポリシーでは、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するターゲットデバイスを指定します。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、または侵入および検出データがないかトラフィックを検査するようにこのデフォルトアクションを設定できます。



インライン展開されたデバイス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、インライン設定をパッシブに展開されたデバイスに適用することがシステムによって阻害されます。

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、この章には、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。詳細については、以下を参照してください。

- [アクセスコントロールのライセンスおよびロール要件\(12-2 ページ\)](#)
- [基本的なアクセスコントロールポリシーの作成\(12-6 ページ\)](#)
- [アクセスコントロールポリシーの管理\(12-12 ページ\)](#)
- [アクセスコントロールポリシーの編集\(12-13 ページ\)](#)
- [失効したポリシーの警告について\(12-16 ページ\)](#)
- [アクセスコントロールポリシーの適用\(12-17 ページ\)](#)
- [IPS または検出のみのパフォーマンスの考慮事項\(12-23 ページ\)](#)

- [アクセスコントロールポリシーおよびルールのトラブルシューティング\(12-25 ページ\)](#)
- [現在のアクセスコントロール設定のレポートの生成\(12-30 ページ\)](#)
- [アクセスコントロールポリシーの比較\(12-31 ページ\)](#)

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ラックリスト登録することができます。さらに、アクセスコントロールルールを使用して、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でも複雑でもかまいません。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。アクセスコントロールポリシーの詳細設定オプションでは、復号、前処理、パフォーマンス、およびその他の一般設定を制御できます。

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ブラックリスト登録\(13-1 ページ\)](#)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即座にブラックリスト登録(ブロック)する方法について説明します。
- [トラフィック復号の概要\(19-1 ページ\)](#)では、SSL ポリシーを使用して、暗号化されたトラフィックを検査することなくブロックしたり、アクセスコントロールルールに渡す(場合によっては復号した後に)方法について説明します。
- [ネットワーク分析ポリシーおよび侵入ポリシーについて\(23-1 ページ\)](#)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\(14-1 ページ\)](#)では、複数の管理対象デバイスでネットワークトラフィックを処理する詳細な方法が、アクセスコントロールルールによっていかに定められるか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\(18-1 ページ\)](#)では、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。この防衛ラインは、トラフィックがその宛先に到達する前に、侵入、禁止されたファイル、およびマルウェアを検出してブロックする(オプション)ことによって実現します。

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ポリシーは、Defense Center のどのライセンスでも作成できますが、多くの機能では、ポリシーを適用する前に適切なライセンスを有効にする必要があります。また、一部の機能は、特定のモデルでのみ使用できます。

また、使用可能なアクセスコントロールに関連する機能とアクションは、ユーザロールによって異なることに注意してください。さまざまな管理者やアナリスト用のユーザロールが事前定義されていますが、それ以外にも特殊なアクセス権限を持たせたカスタムユーザロールを作成できます。

詳細については、以下を参照してください。

- [アクセスコントロールのライセンスおよびモデルの要件\(12-3 ページ\)](#)
- [カスタムユーザロールによる展開の管理\(12-4 ページ\)](#)

アクセスコントロールのライセンスおよびモデルの要件

アクセスコントロールポリシーは、Defense Center でのライセンスに関係なく作成できます。ただし、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ターゲットデバイスで特定のライセンス交付対象の機能を有効化する必要があります。また、一部の機能は、特定のモデルでのみ使用できます。

展開環境でサポートされていない機能は、警告アイコンおよび確認ダイアログボックスに示されます。詳細については、警告アイコンの上にポインタを置き、[アクセスコントロールポリシーおよびルールトラブルシューティング \(12-25 ページ\)](#) を参照してください。

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およびアプライアンスモデル要件の説明があります。シリーズ 2 デバイスは、ほとんどの Protection 機能を自動的に有効にするため、デバイスで明示的に Protection を有効にする必要はありません。

表 12-1 アクセスコントロールのライセンスおよびモデルの要件

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	サポートされる Defense Center	サポートされるデバイス
ゾーン、ネットワーク、VLAN、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	Any	Any	任意 (Any)、ただし次を除く。 <ul style="list-style-type: none"> シリーズ 2 デバイスは、URL フィルタリングを実行できません ASA FirePOWER デバイスは、VLAN フィルタリングを実行できません
SSL インспекションを実行する (表 12-2 (12-4 ページ) を参照)	Any	任意。例外として、DC500 はネットワーク、アプリケーション、および SSL 関連の制御に限定されています	シリーズ 3
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	FireSIGHT	DC500 を除くいずれか	シリーズ 3 最大で ASA FirePOWER
侵入検知および侵入防御、ファイル制御、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	Protection	Any	任意: 例外として、シリーズ 2 デバイスで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できません。
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	Malware	DC500 を除くいずれか	シリーズ 2 と X-シリーズを除くすべて
ユーザ制御またはアプリケーション制御を実行する	Control	任意: 例外として、DC500 ではユーザ制御を実行できません。	シリーズ 2 と X-シリーズを除くすべて
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	URL Filtering	DC500 を除くいずれか	すべて (シリーズ 2 を除く)

■ アクセスコントロールのライセンスおよびロール要件

次の表では、SSL ポリシーを呼び出すことで SSL インспекションを実行するアクセスコントロールポリシーの適用が必要なライセンスについて説明します。

表 12-2 SSL インспекションのライセンスとモデルの要件

SSL ポリシーの機能	ライセンス	サポートされる Defense Center	サポートされるデバイス
ゾーン、ネットワーク、VLAN、ポート、または SSL 関連の条件に基づいて暗号化トラフィックを処理する	Any	Any	シリーズ 3
位置情報のデータを使用して暗号化トラフィックを処理する	FireSIGHT	任意(DC500 を除く)	シリーズ 3
アプリケーションまたはユーザの条件を使用して暗号化トラフィックを処理する	Control	任意:例外として、DC500 ではユーザ制御を実行できません。	シリーズ 3
URL カテゴリおよびレピュテーションデータを使用して暗号化されたトラフィックをフィルタ処理する	URL Filtering	DC500 を除くいずれか	シリーズ 3

カスタム ユーザ ロールによる展開の管理

ライセンス:機能に応じて異なる

[カスタム ユーザ ロールの管理 \(61-56 ページ\)](#) で説明しているように、カスタム ユーザ ロールを作成して専用のカスタム特権を割り当てることができます。カスタム ユーザ ロールには、メタデータベースのアクセス許可およびシステム アクセス許可の任意のセットを割り当てることができます。また、最初から独自に作成したり、事前定義されたユーザ ロールを基に作成したりできます。アクセスコントロール関連の機能に対するカスタム ロールにより、ユーザがアクセスコントロールポリシー、侵入ポリシー、ファイルポリシーを表示、変更、適用できるかどうか、また、管理者ルール カテゴリまたはルートルール カテゴリのルールを挿入または変更できるかどうかが決まります。

次の表に、FireSIGHT システムユーザが操作できるアクセスコントロール関連の機能を決定する、5 つのカスタム ロールの例を記載します。この表には、各カスタム ロールに必要な権限が、カスタム ユーザ ロールを作成するときに表示される順で一覧化されています。

表 12-3 アクセスコントロールのカスタム ロールの例

カスタム ロールの権限	アクセスコントロールおよび SSL エディタ	侵入およびネットワーク分析エディタ	ファイルポリシーエディタ	ポリシーの適用者(すべて)	侵入ポリシーの適用者
アクセス制御	Yes	No	No	Yes	Yes
アクセスコントロールリスト	Yes	No	No	Yes	Yes
アクセス制御ポリシーの変更 (Modify Access Control Policy)	Yes	No	No	No	No
[侵入ポリシーの適用 (Apply Intrusion Policies)]	No	No	No	Yes	Yes

表 12-3 アクセスコントロールのカスタム ロールの例(続き)

カスタム ロールの権限	アクセス コントロールおよび SSL エディタ	侵入およびネットワーク分析エディタ	ファイル ポリシー エディタ	ポリシーの適用者(すべて)	侵入ポリシーの適用者
アクセス コントロール ポリシーの適用 (Apply Access Control Policies)	No	No	No	Yes	No
侵入(ネットワーク分析権限も付与されます)	No	Yes	No	No	No
侵入ポリシー (Intrusion Policy)	No	Yes	No	No	No
[侵入ポリシーの変更 (Modify Intrusion Policy)]	No	Yes	No	No	No
ファイル ポリシー	No	No	Yes	No	No
ファイル ポリシーの変更 (Modify File Policy)	No	No	Yes	No	No
SSL	Yes	No	No	No	No
SSL ポリシーの変更 (Modify SSL Policy)	Yes	No	No	No	No
SSL ポリシーの適用 (Apply SSL Policy)	No	No	No	Yes	No

ただし、FireSIGHT システム のユーザ アカウントのロールが侵入ポリシーまたは修正侵入ポリシーに限定されている場合は、ネットワーク分析ポリシーに加えて、侵入ポリシーを作成して編集できます。

システムがレンダリングする Web インターフェイスは、ユーザが完全なアクセス コントロール ポリシー (侵入ポリシーを含む) を適用できるか、侵入ポリシーのみを適用できるか、あるいはいずれも適用できないかによって異なります。たとえば、上記の表の「侵入ポリシーの適用者」には、アクセス コントロール ポリシーの表示と侵入ポリシーの適用が許可されますが、いずれの編集もできません。また、アクセス コントロール ポリシーを適用することはできず、ファイル ポリシーまたは SSL ポリシーを表示することもできません。この場合、Web インターフェイスでは、

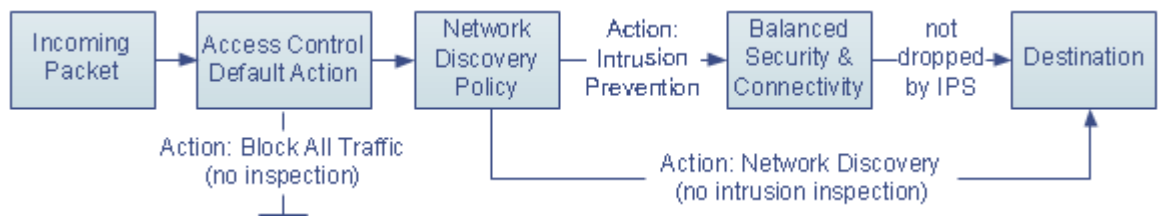
- [アクセス コントロール ポリシー (Access Control Policy)] ページで、編集アイコン(✎)は表示されません
- [アクセス コントロール ポリシー (Access Control Policy)] ページで、削除アイコン(🗑)は表示されません
- クイック適用のポップアップ ウィンドウは、侵入ポリシーだけに適用されます
- 詳細適用ポップアップ ウィンドウで、アクセス コントロール ポリシーのチェックボックスが無効になります

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(Any)

新しいアクセスコントロールポリシーを作成する際には、そのポリシーに一意的な名前を付けて、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では、ポリシーのターゲットデバイスがすべての非高速パスを通るトラフィックを処理する方法が決まります。後でトラフィックフローに影響する他の設定を追加します。ポリシーの作成時にポリシーターゲットを特定する必要はありませんが、ポリシーを適用する前に、このステップを実行する必要があります。

新しいポリシーを作成する際、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、または侵入および検出データの有無についてトラフィックを検査するかを、デフォルトアクションとして設定できます。



ヒント

初めてアクセスコントロールポリシーを作成する場合は、トラフィックを信頼することをデフォルトアクションとして選択できません。デフォルトですべてのトラフィックを信頼する場合は、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、[アクセスコントロールポリシー(Access Control Policy)] ページ([ポリシー(Policies)] > [アクセスコントロール(Access Control)]) を使用します。Defense Center にデバイスを登録しているかどうか、およびその登録方法に応じて、2つの事前定義済みアクセスコントロールポリシーのいずれかが表示され、デバイスにすでに適用されている場合があります。

- デフォルトのアクセスコントロールポリシーでは、追加のインスペクションなしですべてのトラフィックがブロックされます。
- デフォルトの侵入防御ポリシーでは、すべてのトラフィックが許可されますが、Balanced Security and Connectivity 侵入ポリシーおよびデフォルトの侵入変数セットを使用して検査も実行します。

これらのアクセスコントロールポリシーのいずれかを使用および変更できます。これらのデフォルトポリシーでは、ロギングが有効になっていないことに注意してください。



注意

アクセスコントロールポリシーを初めて適用する際、Snort プロセスが再起動し、一時的にトラフィックのインスペクションを中断します。この中断中にトラフィックがドロップされるか、それ以上インスペクション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。詳細については、[Snort の再開によるトラフィックへの影響\(1-9 ページ\)](#)を参照してください。

アクセスコントロールポリシーの作成方法:

アクセス: Admin/Access Admin/Network Admin

- 手順 1 [ポリシー(Policies)] > [アクセス制御(Access Control)] を選択します。
[アクセスコントロールポリシー(Access Control Policy)] ページが表示されます。



ヒント この Defense Center から既存のポリシーをコピーするか、または他の Defense Center からポリシーをインポートすることもできます。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\(A-1 ページ\)](#)を参照してください。

- 手順 2 [新しいポリシー(New Policy)] をクリックします。
[新しいアクセスコントロールポリシー(New Access Control Policy)] ポップアップウィンドウが表示されます。
- 手順 3 [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。
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が、番号記号(#)、セミコロン(;)、または波カッコ({}) 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。
- 手順 4 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。
 - [ネットワーク検出(Network Discovery)] で、[ネットワーク検出のみ(Network Discovery Only)] をデフォルトアクションとして使用するポリシーを作成します。
- 初期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、[ネットワークトラフィックに対するデフォルトの処理とインスペクションの設定\(12-8 ページ\)](#)を参照してください。
- 手順 5 [使用可能なデバイス(Available Devices)] から、ポリシーを適用するデバイスを選択します。
複数のデバイスを選択するには、Ctrl キーまたは Shift キーを押しながらクリックするか、または右クリックをして [すべて選択(Select All)] を選択します。表示されるデバイスを絞り込むには、[検索(Search)] フィールドに検索文字列を入力します。ターゲットデバイスの追加を省略する場合は、後でそれらを追加する方法について、[アクセスコントロールポリシーのターゲットデバイスの設定\(12-10 ページ\)](#)を参照してください。
- 手順 6 [ポリシーに追加(Add to Policy)] をクリックして、選択したデバイスを追加します。
選択したオブジェクトをドラッグアンドドロップすることもできます。
- 手順 7 [保存(Save)] 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\(12-13 ページ\)](#)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。[アクセスコントロールポリシーの適用\(12-17 ページ\)](#)を参照してください。

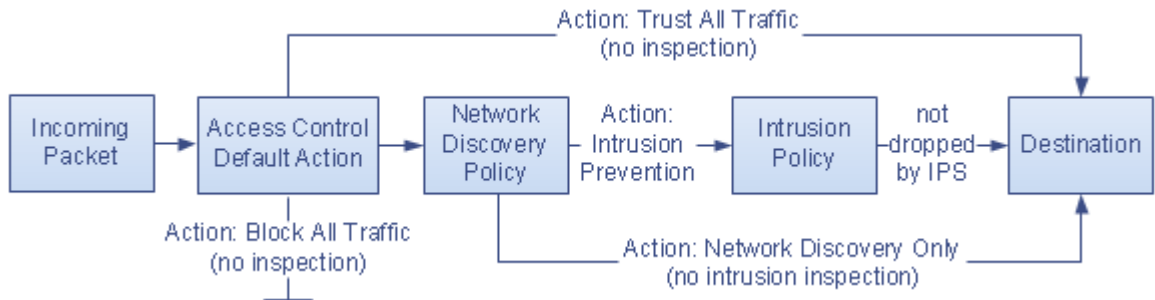
ネットワークトラフィックに対するデフォルトの処理とインスペクションの設定

ライセンス:任意(Any)

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では、次のトラフィックをシステムで処理する方法が決まります。

- セキュリティインテリジェンスによってブラックリスト登録されていないトラフィック
- SSLインスペクションによってブロックされていないトラフィック(暗号化トラフィックのみ)
- ポリシー内のどのルールにも一致しないトラフィック(トラフィックの照合とロギングは行うが、処理または検査はしないモニタールールを除く)

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、または侵入および検出データの有無について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に対しては、ファイルやマルウェアのインスペクションを実行できないので注意してください。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\(18-1 ページ\)](#)を参照してください。

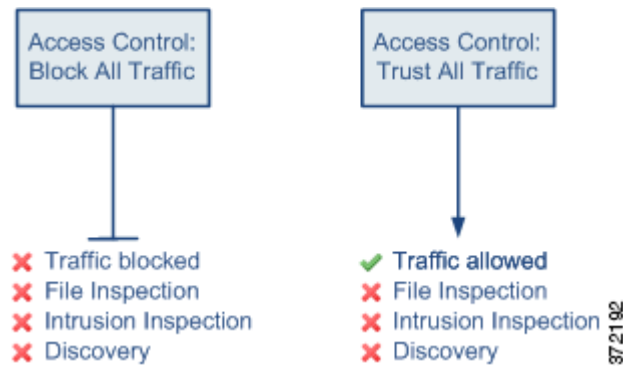
表 12-4 アクセスコントロールポリシーのデフォルトアクション

デフォルトアクション	トラフィックに対して行う処理	インスペクションタイプとポリシー
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	それ以上のインスペクションは行わずにブロックする	none
アクセスコントロール:すべてのトラフィックを信頼	信頼(追加のインスペクションなしで最終宛先に許可)	none

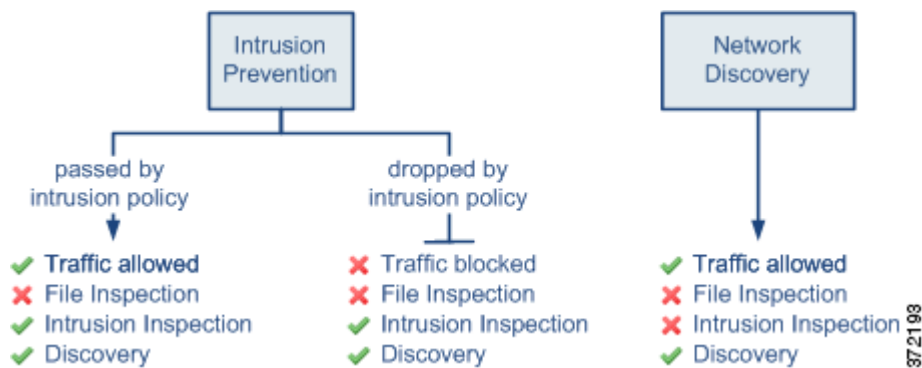
表 12-4 アクセスコントロールポリシーのデフォルトアクション(続き)

デフォルトアクション	トラフィックに対して行う処理	インスペクションタイプとポリシー
侵入防御(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が必要)	侵入 (intrusion)、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、および 検出 (discovery)、ネットワーク検出ポリシーを使用
ネットワーク検出のみ (Network Discovery Only)	許可 (allow)	検出のみ (discovery only)、ネットワーク検出ポリシーを使用

次の図は、[すべてのトラフィックをブロック (Block All Traffic)] および [すべてのトラフィックを信頼 (Trust All Traffic)] デフォルトアクションを示しています。



次の図は、[侵入防御 (Intrusion Prevention)] および [ネットワーク検出のみ (Network Discovery Only)] のデフォルトアクションを説明しています。



ヒント

[ネットワーク検出のみ (Network Discovery Only)] の目的は、検出のみの展開でパフォーマンスを向上させることです。侵入の検知および防御のみを目的としている場合は、さまざまな設定で検出を無効にできます。他の順守の必要なガイドラインなどの詳細については、[IPS または検出のみのパフォーマンスの考慮事項 \(12-23 ページ\)](#) を参照してください。

初めてアクセスコントロールポリシーを作成する際には、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ります。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、デフォルトの侵入変数セットが選択した侵入ポリシーに自動的に関連付けられます。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。

アクセス:Admin/Access Admin/Network Admin

-
- 手順 1** [ポリシー (Policies)] > [アクセス制御 (Access Control)] を選択します。
[アクセスコントロールポリシー (Access Control Policy)] ページが表示されます。
- 手順 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。
- 手順 3** [デフォルトアクション (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、[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)] を選択します。
 - すべてのトラフィックを信頼する場合は、[アクセスコントロール:すべてのトラフィックを信頼 (Access Control: Trust All Traffic)] を選択します。
 - すべてのトラフィックを許可し、ネットワーク検出を使用して検査する場合は、[ネットワーク検出のみ (Network Discovery Only)] を選択します。
 - すべてのトラフィックをネットワーク検出と侵入ポリシーの両方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。
- 手順 4** 侵入防御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、設定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、[変数セットの使用 \(3-19 ページ\)](#) を参照してください。
- 手順 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。
デフォルトアクションによっては、一致する接続をその開始、終了、またはその両方でログに記録できます。接続は、Defense Center データベース、外部のシステム ログ (Syslog) または SNMP トラップ サーバに記録できます。詳細については、[アクセスコントロールのデフォルトアクションによって処理された接続のロギング \(38-20 ページ\)](#) を参照してください。
-

アクセスコントロールポリシーのターゲットデバイスの設定

ライセンス:任意 (Any)

アクセスコントロールポリシーを適用するには、その前に、ポリシーを適用する管理対象デバイスを特定する必要があります。ポリシーを適用するデバイスは、ポリシーの作成時に特定できます。または、後で追加することもできます。

次の表では、対象のデバイスを管理する場合に実行可能な操作の概要を説明しています。

表 12-5 対象のデバイスの管理アクション

目的	操作
使用可能なデバイスのリストを検索する	検索フィールド内をクリックして、検索文字列を入力します。検索文字列を入力すると、デバイスのリストが更新されて、検索文字列に一致するデバイス名が表示されます。
使用可能なデバイスの検索をクリアする	検索フィールドのクリアアイコン(✕)をクリックします。
使用可能なデバイスを選択し、選択済みターゲットのリストに追加する	デバイス名をクリックします。複数のデバイスを選択するには、Ctrl キーまたは Shift キーを押しながらクリックします。使用可能なデバイスを右クリックして、[すべて選択 (Select All)] をクリックすることもできます。
選択したデバイスを追加する	[ポリシーに追加 (Add to Policy)] をクリックするか、または選択されたデバイスのリストにドラッグアンドドロップします。
選択済みデバイスのリストから単一のデバイスを削除する	デバイスの横にある削除アイコン(🗑️)をクリックするか、またはデバイスを右クリックし、[削除 (Delete)] を選択します。
選択済みデバイスのリストから複数のデバイスを削除する	Ctrl キーまたは Shift キーを押しながら複数のデバイスをクリックして選択したら、選択したデバイスの行を右クリックして強調表示し、次に [選択項目の削除 (Delete Selected)] をクリックします。

異なるバージョンのシステムを実行中のスタック構成のデバイスをターゲットにすることはできません(たとえば、デバイスのいずれかでアップグレードが失敗した場合)。デバイス スタックをターゲットにすることはできますが、スタック内の個々のデバイスをターゲットにすることはできません。詳細については、[スタック構成のデバイスの管理\(4-47 ページ\)](#)を参照してください。

アクセスコントロールポリシーのターゲット デバイスを管理する方法:

アクセス: Admin/Access Admin/Network Admin

-
- 手順 1 [ポリシー (Policies)] > [アクセス制御 (Access Control)] を選択します。
[アクセスコントロールポリシー (Access Control Policy)] ページが表示されます。
- 手順 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。
- 手順 3 デバイス ターゲットのリンクをクリックし、[ターゲットの管理 (Manage Targets)] をクリックします。
[デバイス ターゲットの管理 (Manage Device Targets)] ポップアップ ウィンドウが表示されます。
- 手順 4 ターゲット リストを作成します。
[表 12-5\(12-11 ページ\)](#)に要約されているアクションを使用します。
- 手順 5 [OK] をクリックします。
設定がポリシーに追加され、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。
-

アクセスコントロールポリシーの管理

ライセンス:任意(Any)






[アクセスコントロールポリシー(Access Control Policy)] ページ([ポリシー(Policies)]>[アクセスコントロール(Access Control)])で、現在のカスタムアクセスコントロールポリシーを次の情報とともに(適切な場合)表示できます。

- トラフィックの検査に各アクセスコントロールポリシーを使用しているデバイスの数。ポリシーがそのターゲットの一部にのみ適用されているか、またはそのポリシーが現在ターゲットとしていないデバイスに適用されているかに関する情報も含まれます。
- 各ポリシーが失効しているターゲット デバイスの数、および各ポリシーを現在編集している人に関する情報(いる場合)。

作成したカスタムポリシーに加えて、システムによって3つのカスタムポリシー(デフォルトのアクセスコントロールポリシー、デフォルトの侵入防御ポリシー、およびデフォルトのネットワーク検出ポリシー)が提供される場合があります。初期設定時にデバイスで選択した検出モードに応じて、システムでは最初のデバイス登録時にこれらのポリシーが作成されます。これらのシステム付属のカスタムポリシーは編集して使用できます。デバイスの検出モードはユーザが後から変更できない設定で、設定時にユーザが選択するだけのオプションです。このオプションの選択により、システムはデバイスの初期設定を調整することができます。

[アクセスコントロールポリシー(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 12-6 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	[新しいポリシー(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(12-6 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(12-13 ページ)
アクセスコントロールポリシーを管理対象デバイスに再適用する	適用アイコン()をクリックします。	アクセスコントロールポリシーの適用(12-17 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Defense Center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。	設定のエクスポート(A-1 ページ)
アクセスコントロールポリシーの現行の設定を一覧化した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。	現在のアクセスコントロール設定のレポートの生成(12-30 ページ)
アクセスコントロールポリシーを比較する	[ポリシーの比較(Compare Policies)]をクリックします。	アクセスコントロールポリシーの比較(12-31 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。適用されたアクセスコントロールポリシーまたは現在適用しているアクセスコントロール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(Any)

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は、アクセスコントロールポリシーエディタが表示され、[ルール(Rules)]タブがフォーカスされます。次の図は、新たに作成されたポリシーを示しています。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ではすべてのトラフィックが処理されます。この場合、デフォルトアクションは、暗号化されていないトラフィックを最終宛先に許可する前に、システムが提供する **Balanced Security and Connectivity** 侵入ポリシーを使用して検査します。デフォルトでは、システムは暗号化されたペイロードでファイルおよび侵入のインスペクションを無効にするため、注意してください。

Simple Access Control Policy

inspects all traffic with a balanced intrusion policy

The screenshot shows the configuration page for a 'Simple Access Control Policy'. At the top, there are tabs for 'Rules', 'Targets (0)', 'Security Intelligence', 'HTTP Responses', and 'Advanced'. Below the tabs is a search bar with 'Filter by Device', 'Add Category', 'Add Rule', and 'Search Rules' options. The main area is a table with columns: '#', 'Name', 'Src', 'De', 'UR', 'Action', and several icons. The table is currently empty, with a message 'No data to display' at the bottom. The 'Default Action' is set to 'Intrusion Prevention: Balanced Security and Connectivity'. The page number 'Page 1 of 1' is visible at the bottom right.

ルールの追加および整理、ポリシーを使用するデバイスの指定などを行うには、アクセスコントロールポリシーエディタを使用します。次のリストには、変更可能なポリシー設定に関する情報を記載しています。

名前(Name)と説明(Description)

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。

ターゲット(Targets)

アクセスコントロールポリシーを適用するには、その前に [ターゲット(Targets)] タブを使用して、ポリシーを適用する管理対象デバイス(デバイスグループを含む)を特定します。詳細については、[アクセスコントロールポリシーのターゲットデバイスの設定\(12-10 ページ\)](#)を参照してください。

セキュリティインテリジェンス (Security Intelligence)

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、接続を即座にブラックリスト登録(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、ブラックリストはカスタムホワイトリストで上書きできます。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めて、他のどのポリシーベースのインスペクション、分析、トラフィック処理よりも先に行われます。詳細については、[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ブラックリスト登録\(13-1 ページ\)](#)を参照してください。

ルール (Rule)

ルールによって、ネットワークトラフィックをきめ細かく処理することができます。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上から順に、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、VLAN、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およびアプライアンスモデル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、[ルール (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\(14-1 ページ\)](#)を参照してください。

デフォルトアクション (Default Action)

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ラックリスト登録されず、いずれのアクセスコントロール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することができます。また、侵入および検出データの有無についてトラフィックを検査することもできます。また、カスタム変数セットを作成している場合はそれを選択し、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、[ネットワークトラフィックに対するデフォルトの処理とインスペクションの設定\(12-8 ページ\)](#)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\(38-18 ページ\)](#)を参照してください。

HTTP 応答 (HTTP Responses)

ユーザの Web サイト要求がシステムによってブロックされた場合にブラウザに表示するものを指定できます。システム付属の一般的な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、続行するかページを更新して最初に要求したサイトをロードするかを、ボタンをクリックして選択させることもできます。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\(16-21 ページ\)](#)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 (Advanced Access Control Options)

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、Defense Center データベースに保存される文字数。接続で検出された URL のロギング(38-22 ページ)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隔。ブロックされた Web サイトのユーザ バイパス タイムアウトの設定(16-20 ページ)を参照してください。
- 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、復号、ブロック、または許可する SSL ポリシー。アクセス コントロールを使用した復号設定の適用(20-10 ページ)を参照してください
- ポリシー適用時にトラフィック インスペクションを許可する、またはセキュアな接続に対するトラフィック インスペクションを無効にする。アクセス コントロールポリシーの適用(12-17 ページ)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、ゾーン、および VLAN 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。トラフィックの前処理のカスタマイズ(25-1 ページ)を参照してください
- 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。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、ゾーン、および VLAN にグローバルに適用されます。トランスポート/ネットワークの詳細設定の構成(29-2 ページ)を参照してください
- 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。パッシブ展開における前処理の調整(30-1 ページ)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、ファイル ストレージ、ダイナミック分析、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(18-10 ページ)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(18-21 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、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、[アクセスコントロールポリシー (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。

2 つのブラウザ ウィンドウで同じポリシーを編集しようとする、新しいウィンドウで編集を再開するか、元のウィンドウでの変更を破棄して新しいウィンドウで編集を続けるか、または 2 番目のウィンドウをキャンセルしてポリシー エディタに戻るかを選択するよう求めるプロンプトが出されます。

複数のユーザが同じポリシーを同時に編集する際、各ユーザに対し、ポリシー エディタにメッセージが表示され、他のユーザによる未保存の変更があることが通知されます。いずれかのユーザが変更を保存しようとする、その変更が他のユーザの変更を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。

アクセスコントロールポリシーの編集方法:

アクセス:Admin/Access Admin/Network Admin

-
- 手順 1 [ポリシー(Policies)] > [アクセス制御(Access Control)] を選択します。
[アクセスコントロールポリシー(Access Control Policy)] ページが表示されます。
- 手順 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。
- 手順 3 ポリシーを編集します。上に概要を示したいいずれかのアクションを実行します。
- 手順 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、[保存(Save)] をクリックします。
 - 変更を保存し、ポリシーを適用する場合は、[保存して適用(Save and Apply)] をクリックします。[アクセスコントロールポリシーの適用\(12-17 ページ\)](#)を参照してください。
 - 変更を廃棄する場合は、[キャンセル(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(Any)

[アクセスコントロールポリシー(Access Control Policy)] ページ([ポリシー(Policies)] > [アクセスコントロール(Access Control)]) で、失効したポリシーには、ポリシーの更新に必要なターゲットデバイスの数を示した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ときは、変更を有効にするためにそのポリシーを再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したりする場合、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、ポリシーターゲット、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です。
- 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。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です。
- 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、VLAN タグ、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ルド、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、復号関連オブジェクト、セキュリティゾーンなどです。
- 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。

Web インターフェイスの複数の場所からこれらの設定の一部を変更できることに留意してください。たとえば、オブジェクトマネージャ ([オブジェクト (Objects)] > [オブジェクト管理 (Object Management)]) を使用してセキュリティゾーンを変更できますが、デバイスの設定 ([デバイス (Devices)] > [デバイス管理 (Device Management)]) でインターフェイスのタイプを変更すると、ゾーンも変更され、ポリシーの再適用が必要になります。

次の更新では、ポリシーの再適用は必要ありません。

- セキュリティインテリジェンス フィードへの自動更新およびコンテキストメニューを使用したセキュリティインテリジェンスのグローバルブラックリストおよびホワイトリストへの追加
- 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。

アクセス: Admin/Security Approver

-
- 手順 1** [ポリシー (Policies)] > [アクセス制御 (Access Control)] を選択します。
[アクセスコントロールポリシー (Access Control Policy)] ページが表示されます。失効したポリシーには、ポリシーの更新を必要とするターゲットデバイスの数を示した赤色のステータステキストが付いています。
 - 手順 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 [アクセスコントロールポリシーの適用 (Apply Access Control Policy)] ポップアップウィンドウが表示されます。
 - 手順 3** 該当する変更されたコンポーネントの横にある [失効 (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の比較 \(12-31 ページ\)](#) および [2 つの侵入ポリシーまたはリビジョンの比較 \(31-11 ページ\)](#) を参照してください。
 - 手順 4** オプションで、ポリシーを再度適用します。
次の項、[アクセスコントロールポリシーの適用](#) を参照してください。
-

アクセスコントロールポリシーの適用

ライセンス: 任意 (Any)

アクセスコントロールポリシーを変更した後、そのポリシーを 1 つ以上のターゲットデバイスに適用することで、デバイスがモニタ対象とするネットワークでその変更を実装できます。アクセスコントロールポリシーおよび関連する侵入ポリシーは任意の組み合わせで適用することができますが、アクセスコントロールポリシーを適用すると、そのポリシーに関連付けられたすべての SSL ポリシー、ネットワーク分析ポリシー、およびファイルポリシーが自動的に適用されます。これらのポリシーを個別に適用することはできません。

**注意**

アクセスコントロールポリシーの適用時に、リソース需要が生じる結果として、少数のパケットがインスペクションなしでドロップされることがあります。さらに、構成の一部を適用するときに、Snort プロセスの再開が要求され、これにより一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクション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。[Snort の再開によるトラフィックへの影響\(1-9 ページ\)](#)を参照してください。

**ヒント**

インラインで Blue Coat X-Series 向け Cisco NGIPS を展開していて、ロードバランシングおよび冗長性のためにマルチ VAP VAP グループを設定している場合、デバイスが再起動するまで影響を受ける VAP をロードバランス リストから削除し、再起動した後に再インストールすることで、処理の中断を防ぐことができます。

インライン展開されたデバイス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。たとえば、ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。

場合によっては、タップモードのインラインデバイスを含むパッシブに展開されたデバイスにインライン設定を適用することが、システムによって阻害されます。たとえば、パッシブ展開では、暗号化されたトラフィックをブロックする SSL ポリシー、または復号されたトラフィックに再署名するよう設定された SSL ポリシーを参照するアクセスコントロールポリシーを適用することはできません。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がサポートされません。

アクセスコントロールポリシーを適用する際には、次の点に注意してください。

- 一部の機能には、特定のライセンス、最小バージョンのシステム、または特定のデバイスモデルが必要です。詳細については、[アクセスコントロールのライセンスおよびモデルの要件\(12-3 ページ\)](#)と、管理対象デバイスで実行しているシステムのバージョンのリリースノート参照してください。アクセスコントロールポリシーが最も新たに適用されたデバイス設定を介して有効になるライセンスを必要とする場合、システムはそのデバイス設定の適用が完了するまで、アクセスコントロールポリシー適用タスクをキューに入れておきます。
- 異なるバージョンのシステムを実行しているスタックデバイスに、アクセスコントロールポリシーを適用することはできません(たとえば、デバイスの1つでアップグレードが失敗した場合など)。
- 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ターゲットデバイスが使用する拡張基準セットを作成します。ターゲットデバイスで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。この最大値は、デバイスの物理メモリやプロセッサ数などの、さまざまな要因によって異なります。コンピューティングリソースが少ないデバイスでは、メモリの制約上、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ので注意してください。詳細については、[パフォーマンスを向上させるためのルールの簡素化\(12-26 ページ\)](#)を参照してください。

- アプリケーション制御を実行する場合は、アクセスコントロールルールまたはSSLルールで条件として使用するアプリケーションごとに少なくとも1つのディテクタを有効にする必要があります。あるアプリケーションのディテクタが1つも有効になっていない場合、システムは、そのアプリケーションに関するシステム提供のディテクタをすべて自動的に有効化します。それが1つも存在しない場合は、そのアプリケーション用の最後に変更されたユーザ定義ディテクタが有効化されます。
- 侵入ルールの更新をインポートすると、インポートの完了後にアクセスコントロールポリシーと侵入ポリシーを自動的に再適用できます。これにより、最新の侵入ルールと詳細設定だけでなく、プリプロセッサルールとプリプロセッサ設定も使用できるようになります。これは、ルールの更新によってシステム付属の基本ポリシーが変更されることを許可する場合に特に役立ちます。ただし、ルールの更新によって、アクセスコントロールポリシーの前処理およびパフォーマンスの詳細設定オプションのデフォルト値が変更されることがあります。詳細については、[ルールの更新とローカルルールファイルのインポート\(66-16 ページ\)](#)を参照してください。
- メモリが制限されているデバイスでは、侵入ポリシーの数が、複数の変数セットとペアにならない可能性があります。1つの侵入ポリシーのみを参照するアクセスコントロールポリシーを適用できる場合は、この侵入ポリシーに対するすべての参照が、同一の変数セットとペアになっていることを確認してください。

詳細については、次の各項を参照してください。

- [ポリシー全体の適用\(12-19 ページ\)](#)では、クイック適用オプションを使用して、関連するすべてのSSLポリシー、ネットワーク分析ポリシー、侵入ポリシー、ファイルポリシーと併せて、アクセスコントロールポリシーを適用する方法について説明しています。
- [選択したポリシーの設定の適用\(12-20 ページ\)](#)では、個々の侵入ポリシーを含む、特定のアクセスコントロールポリシー設定を適用する方法について説明しています。

ポリシー全体の適用

ライセンス:任意(Any)

サポートされるデバイス:

アクセスコントロールポリシーは、いつでもターゲットデバイスに適用することができます。アクセスコントロールポリシーを適用すると、以下の関連ポリシーも、現在実行しているものとは異なる設定で適用されます。

- SSLポリシー
- 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

ポップアップウィンドウを使用すると、単一のクイック適用操作としてすべてのポリシーをまとめて適用できます。クイック適用オプションを使用する場合、変更されていないポリシーは適用されません。

クイック適用ポップアップウィンドウの適用ボタンのラベルは、アクセスコントロールポリシー、侵入ポリシー、またはその両方の適用を許可されているかによって異なります。[カスタムユーザロールによる展開の管理\(12-4 ページ\)](#)を参照してください。

アクセスコントロールポリシー全体をクイック適用するには、次の手順を実行します。

アクセス:Admin/Security Approver

-
- 手順 1** [ポリシー (Policies)] > [アクセス制御 (Access Control)] を選択します。
[アクセスコントロールポリシー (Access Control Policy)] ページが表示されます。
- 手順 2** 適用するポリシーの横にある適用アイコン(☑)をクリックします。
[アクセスコントロールポリシーの適用 (Apply Access Control Policy)] ポップアップウィンドウが表示されます。
または、ポリシーの編集中に [保存して適用 (Save and Apply)] をクリックできます。[アクセスコントロールポリシーの編集 \(12-13 ページ\)](#) を参照してください。
- 手順 3** [すべて適用 (Apply All)] をクリックします。
ポリシー適用タスクがキューに入れられます。[OK] をクリックして [アクセスコントロールポリシー (Access Control Policy)] ページに戻ります。ポリシー適用タスクの進行状況は、[タスクステータス (Task Status)] ページ ([システム (System)] > [モニタリング (Monitoring)] > [タスクステータス (Task Status)]) でモニタできます。
-

選択したポリシーの設定の適用

ライセンス:任意 (Any)

ポリシー適用の詳細ページを使用して、アクセスコントロールポリシーや関連する侵入ポリシーに変更を適用できます。詳細ページには、ポリシーの対象となるデバイスが一覧表示され、デバイス別のアクセスコントロールポリシーのカラム、および関連する侵入ポリシーのカラムが表示されます。ターゲットデバイスごとに、変更をアクセスコントロールポリシー、関連する個別または組み合わせの侵入ポリシー、あるいはその両方に適用するかどうかを指定できます。

次の場合には、アクセスコントロールポリシーとその関連侵入ポリシーの両方を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初めてデバイスに適用される場合
- アクセスコントロールポリシーに新しく侵入ポリシーが追加される場合

いずれの場合も、アクセスコントロールポリシーの状態と侵入ポリシーの状態はリンクしていません。つまり、両方とも適用するか、どちらも適用しないかのいずれかを選択する必要があります。

どの侵入ポリシーを適用するかに関係なく、アクセスコントロールポリシーを適用すると、そのポリシーの対象デバイスで現在実行されているポリシーとは異なる、関連する SSL ポリシー、ネットワーク分析ポリシー、ファイルポリシーがすべて自動的に適用されます。これらのポリシーを個別に適用することはできません。

[アクセスコントロールポリシー (Access Control Policy)] カラム

[アクセスコントロールポリシー (Access Control Policy)] カラムには、アクセスコントロールポリシーを適用するかどうかを指定するチェックボックスがあります。



ヒント

タスクキューにまだ入っているポリシー、つまり適用タスクがまだ完了していないポリシーを再び適用することもできますが、それには何の利点もありません。

ステータスメッセージには、ポリシーが現在最新の状態であるか、失効しているかどうかを示されます。ポリシーが失効している場合は、新しいブラウザ ウィンドウで、そのポリシーと現在実行中のポリシーとの比較結果を表示できます。この比較には、アクセスコントロールポリシーに関連付けられている侵入ポリシーでの差異は含まれません。

[侵入ポリシー (Intrusion Policies)] カラム

[侵入ポリシー (Intrusion Policies)] カラムには 1 つ以上のチェック ボックスがあり、アクセスコントロールポリシーに関連する侵入ポリシーをデバイスに適用するかどうかを指定できます。単一のグレー表示されたチェック ボックスは、関連付けられているすべての侵入ポリシーが、現在実行されているポリシーと同じであることを意味します。この場合、チェック ボックスはクリアされていて、選択することはできません。変更されていない侵入ポリシーを適用することはできません。このカラムには、変更されている侵入ポリシーだけがリストされ、個別に選択できるようになっています。ポリシーに含まれる複数のルールに同じ侵入ポリシーが関連付けられている場合、その侵入ポリシーはデバイスごとに一度だけリストされます。

前述したようにアクセスコントロールポリシーと侵入ポリシーを一緒に適用しなければならない場合、侵入ポリシーのチェック ボックスは選択された状態でグレー表示され、変更することができません。これに該当するのは次のような場合です。

- アクセスコントロールポリシーが初めてデバイスに適用される場合
- アクセスコントロールポリシーに新しく侵入ポリシーが追加される場合

ステータスメッセージには、侵入ポリシーが現在最新の状態であるか、失効しているかどうかを示されます。侵入ポリシーが、リスト内のデバイスで現在実行されている侵入ポリシーと異なる場合、その侵入ポリシーは失効していることとなります。侵入ポリシーがデバイス上の侵入ポリシーとまったく同じであれば、その侵入ポリシーは最新の状態です。ポリシーが失効している場合は、新しいブラウザ ウィンドウで、そのポリシーと現在実行中のポリシーとの比較結果を表示できます。

選択したアクセスコントロールポリシー設定を適用する方法:

アクセス:Admin/Security Approver

-
- 手順 1** [ポリシー (Policies)] > [アクセス制御 (Access Control)] を選択します。
[アクセスコントロールポリシー (Access Control Policy)] ページが表示されます。
 - 手順 2** 適用するポリシーの横にある適用アイコン (✓) をクリックします。
[アクセスコントロールポリシーの適用 (Apply Access Control Policy)] ポップアップ ウィンドウが表示されます。
または、ポリシーの編集に [保存して適用 (Save and Apply)] をクリックできます。[アクセスコントロールポリシーの編集 \(12-13 ページ\)](#) を参照してください。
 - 手順 3** [詳細 (Details)] をクリックします。
詳細な [アクセスコントロールポリシーの適用 (Apply Access Control Policy)] ポップアップ ウィンドウが表示されます。このポップアップ ウィンドウは、[アクセスコントロールポリシー (Access Control Policy)] ページ ([ポリシー (Policies)] > [アクセスコントロール (Access Control)]) から開くこともできます。それには、ポリシーの [ステータス (Status)] 列に示されている失効メッセージをクリックします。
 - 手順 4** デバイス名の横にあるアクセスコントロールポリシーのチェック ボックスを選択するかクリアにして、アクセスコントロールポリシーをターゲット デバイスに適用するかどうかを指定します。
 - 手順 5** デバイス名の横にある侵入ポリシーのチェック ボックスを選択またはクリアして、侵入ポリシーをターゲット デバイスに適用するかどうかを指定します。

手順 6 [選択した設定の適用 (Apply Selected Configurations)] をクリックします。

ポリシー適用タスクがキューに入れられます。[OK] をクリックして [アクセスコントロールポリシー (Access Control Policy)] ページに戻ります。

ただし、デバイスでサポートされる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ポリシーを再評価し、侵入ポリシーを統合する必要があります。関連付けられている侵入ポリシーの数 (デフォルトアクションを含む) が最大値以内に収まるまで、アクセスコントロールポリシーは適用できません。

ポリシー適用タスクの進行状況は、[タスクステータス (Task Status)] ページ ([システム (System)] > [モニタリング (Monitoring)] > [タスクステータス (Task Status)]) でモニタできます。

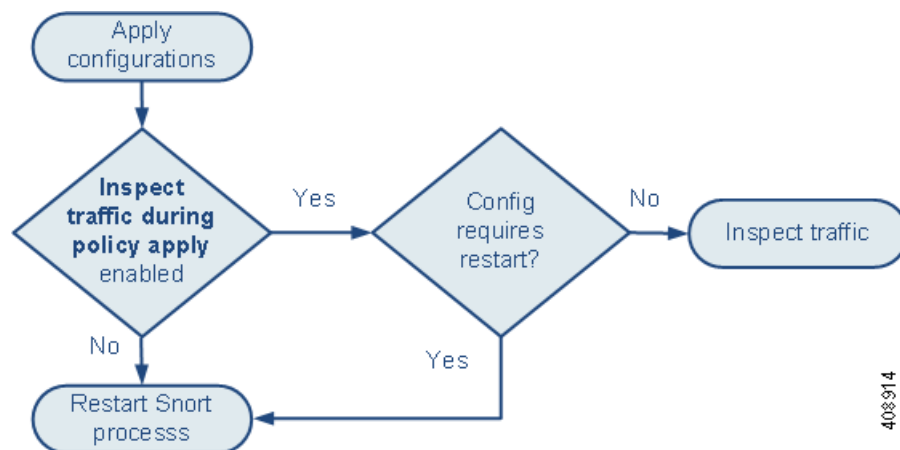
アクセスコントロールポリシー適用中のトラフィックインスペクション

次の図は、拡張アクセスコントロールポリシーオプション [ポリシー適用中のトラフィック検査 (Inspect traffic during policy apply)] を有効または無効にしたときに Snort プロセスがどのように再起動されるかを示しています。



注意

Snort プロセスを再起動すると、一時的にトラフィックインスペクションが中断されます。この中断中にトラフィックがドロップされるか、インスペクション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。[Snort プロセスを再開する構成 \(1-8 ページ\)](#) を参照してください。



408314

次の点に注意してください。

- [ポリシー適用中のトラフィック検査 (Inspect traffic during policy apply)] を有効にした場合は、次のようになります。
 - 一部の構成で、Snort プロセスの再起動が要求されることがあります。
 - 適用した構成で Snort の再起動が要求されない場合、システムはまず最初に、現在適用されているアクセスコントロールポリシーを使用してトラフィックを検査し、アプリケーションプロセス中に、適用されたポリシーに切り替えます。

- [ポリシー適用中のトラフィック検査 (Inspect traffic during policy apply)] を無効にすると、ポリシーを適用する際に必ず Snort プロセスが再起動します。
- Snort の再起動がトラフィックにどのように影響するかは、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。Snort の再開によるトラフィックへの影響 (1-9 ページ) を参照してください。

IPS または検出のみのパフォーマンスの考慮事項

ライセンス: FireSIGHT または Protection

FireSIGHT ライセンスは Defense Center に含まれており、このライセンスによりホスト、アプリケーション、およびユーザのディスカバリを実行できます。検出データを使用して、システムはネットワークの完全な最新プロファイルを作成できます。管理対象デバイスに適用されている Protection ライセンスを使用して、システムは侵入検知と侵入防御システム (IPS) として機能できます。侵入とエクスプロイトの有無についてネットワークトラフィックを分析できます。またオプションで違反パケットをドロップできます。

検出と IPS を組み合わせることで、ネットワークアクティビティにコンテキストが提供され、次のような多くの機能を利用することができます。

- 侵害の影響フラグと兆候。これによって、どのホストが特定のエクスプロイト、攻撃、またはマルウェアに対して脆弱であるかが示されます。
- 適応型プロファイルと FireSIGHT の推奨事項。これを使用して、宛先ホストに応じてトラフィックを個別に検査できます。
- 相関。これによって、影響を受けるホストに応じて別々に侵入 (およびその他のイベント) に応答できます。

ただし、所属する組織が IPS のみまたは検出のみを実行することを目的としている場合は、次のセクションに示すように、システムのパフォーマンスを最適化できる設定がいくつかあります。

- ネットワーク検出のみの展開の最適化 (12-23 ページ)
- 検出なしの侵入検知と防御の実行 (12-24 ページ)

ネットワーク検出のみの展開の最適化

ライセンス: FireSIGHT

検出機能では、ネットワークトラフィックをモニタして、ネットワーク上のホストの数とタイプ (ネットワークデバイスを含む) だけでなく、それらのホスト上のオペレーティングシステム、アクティブなアプリケーション、およびオープンポートを判断できます。管理対象デバイスとユーザエージェントを、ネットワークのユーザアクティビティをモニタするように設定することもできます。検出データを使用して、トラフィックプロファイリングを実行し、ネットワークコンプライアンスを評価し、ポリシー違反に応答できます。

基本的な展開 (検出と単純なネットワークベースのアクセス制御のみ) では、アクセスコントロールポリシーの設定時にいくつかの重要なガイドラインに従うことで、デバイスのパフォーマンスを向上させることができます。



(注)

それが単にすべてのトラフィックを許可する場合であっても、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。ネットワーク検出ポリシーでは、アクセスコントロールポリシーが通過を許可したトラフィックを検査することのみ可能です。

最初に、アクセスコントロールポリシーは複雑な処理を必要とせず、単純なネットワークベースの基準のみを使用してネットワークトラフィックを処理することを確認します。次のすべてのガイドラインを実装する必要があります。これらのオプションのいずれかを誤って設定すると、パフォーマンス上の利点がなくなります。

- セキュリティインテリジェンス機能を使用しないでください。入力されたグローバルホワイトリストまたはブラックリストをポリシーのセキュリティインテリジェンスの設定から削除します。
- モニタアクションまたはインタラクティブブロックアクションに、アクセスコントロールルールを含めないでください。許可、信頼、およびブロックルールのみを使用します。許可されたトラフィックは検出によって検査できますが、信頼されたトラフィックとブロックされたトラフィックは検査できないことに留意してください。
- デバイスが適切なライセンスを取得済みであっても、アプリケーション、ユーザ、URL、または位置情報ベースのネットワーク条件にアクセスコントロールルールを含めないでください。単純なネットワークベースの条件(ゾーン、IP アドレス、VLAN タグ、およびポート)のみを使用します。
- デバイスが適切なライセンスを取得済みであっても、ファイル、マルウェア、または侵入のインスペクションを実行するアクセスコントロールルールを含めないでください。つまり、ファイルポリシーまたは侵入ポリシーをアクセスコントロールルールに関連付けしないでください。
- 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が [アクティブなルールなし (No Rules Active)] に設定されていることを確認します。[アクセスコントロールのデフォルト侵入ポリシーの設定 \(25-1 ページ\)](#) を参照してください。
- ポリシーのデフォルトアクションとして [ネットワーク検出のみ (Network Discovery Only)] を選択します。侵入インスペクションを実行するポリシーのデフォルトアクションを選択しないでください。

位置情報ベースのアクセス制御を除き、上記のオプションには少なくとも 1 つの Protection ライセンスが必要であることを注意してください。FireSIGHT ライセンスが 1 つだけある場合、これらの機能を使用したアクセスコントロールポリシーの適用がシステムによって阻害されます。

アクセスコントロールポリシーを設定して適用した後、ネットワーク検出ポリシーを設定して適用できます。このポリシーは、システムが検出データについて検査をするネットワークセグメント、ポート、およびゾーンを指定し、ホスト、アプリケーション、およびユーザがセグメント、ポート、およびゾーンで検出されるかどうかを指定します。

検出なしの侵入検知と防御の実行

ライセンス:Protection

侵入検知と防御の機能によって、侵入とエクスプロイトの有無についてネットワークトラフィックを分析できます。またオプションで違反パケットをドロップできます。侵入インスペクションを実行するものの、検出データを利用する必要がない場合は、検出を無効にして、デバイスのパフォーマンスを向上させることができます。



(注)

アプリケーション、ユーザ、または URL の制御を実行する場合は、パフォーマンス上の利点を得るために、検出を無効にすることは**できません**。システムが検出データを保存しないようにすることはできますが、システムはそれらの機能を実行するために検出データを収集して検査する必要があります。

検出を無効にするには、次のすべてのガイドラインを実行します。いずれかでも誤って設定すると、パフォーマンス上の利点がなくなります。

- アクセスコントロールポリシーでは、デバイスが適切なライセンスを取得済みであっても、アプリケーション、ユーザ、URL、または位置情報ベースのネットワーク条件にルールを含めないでください。単純なネットワークベースの条件(ゾーン、IP アドレス、VLAN タグ、およびポート)のみを使用します。
- ネットワーク検出ポリシーからすべてのルールを削除します。

アクセスコントロールポリシーを適用してからネットワーク検出ポリシーを適用すると、新しい検出がターゲットデバイスで停止します。システムは、ネットワーク検出ポリシーで指定されたタイムアウト期間に応じて、ネットワークマップ内の情報を段階的に削除します。または、すべての検出データを即座に消去できます。[データベースからの検出データの消去\(B-1 ページ\)](#)を参照してください。

アクセスコントロールポリシーおよびルールのトラブルシューティング

ライセンス:任意(Any)

アクセスコントロールポリシーを適切に設定すること、特に、アクセスコントロールルールを作成して順序付けること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不可欠なタスクです。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てしまう可能性があります。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、[アクセスコントロールのエラーアイコン](#)の表に示すように、警告とエラーを示します。警告、エラー、または情報のテキストを確認するには、マウスのポインタをアイコンの上に置きます。






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 [警告の表示(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 12-7 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 (Details)
	error	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を与えません。</p> <p>たとえば、プリエンプション処理されたルールや、誤った設定(空のオブジェクトグループを使用した条件、一致するアプリケーションが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と一致することがないルールを含むポリシーであっても、適用することができます。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またはデバイスモデルが必要です。アクセスコントロールポリシーは、対象となるターゲットデバイスのみ normally 適用されます。</p>
	情報	<p>情報アイコンは、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を表示します。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、ユーザが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、システムは接続においてアプリケーショントラフィックまたは Web トラフィックを識別するまで、その接続の最初の数パケットと一部のアクセスコントロールルールとの照合をスキップすることがあります。これにより接続を確立することができ、アプリケーションと HTTP 要求を識別できるようになります。詳細については、アプリケーション制御の制約事項(16-8 ページ)および URL の検出とブロッキングの制約事項(16-17 ページ)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を与える可能性があります。

詳細については、以下を参照してください。

- [アクセスコントロールのライセンスおよびロール要件\(12-2 ページ\)](#)
- [パフォーマンスを向上させるためのルールの簡素化\(12-26 ページ\)](#)
- [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\(12-27 ページ\)](#)
- [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\(12-28 ページ\)](#)

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やルールは、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ターゲットデバイスが使用する拡張基準セットを作成します。ターゲットデバイスで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。この最大値は、デバイスの物理メモリやプロセッサ数などの、さまざまな要因によって異なります。

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。

- ルールの作成時には、条件を構成する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は、個々の 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。

ただし、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ません。たとえば、50 個の IP アドレスを 1 つのネットワークオブジェクトに含めて使用することにパフォーマンス的なメリットはなく、条件にこれらの IP アドレスを個別に含めるよりも単に構成上のメリットがあるだけです。

- できる限り、セキュリティゾーンごとに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ゾーンの 1 つにない場合、ルールはそのデバイスのパフォーマンスに影響を与えません。
- ルールを過度に設定しないでください。処理するトラフィックの照合が 1 つの条件で十分な場合には、2 つの条件を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、デバイス上のリソースと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 つのポリシーと見なされます。

デバイスで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 [アクセスコントロールルールが決定される前に使用される侵入ポリシー (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 (Any)

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不可欠です。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、これと同じ問題が生じ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オンの警告について

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。

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。次の例では、最初のルールでの VLAN 範囲に 2番目のルールでの VLAN が含まれるため、最初のルールが 2番目のルールよりも優先して適用されることとなります。

```
Rule 1: allow VLAN 22-33
Rule 2: block VLAN 27
```

次の例では、VLAN が設定されていないルール 1 はあらゆる VLAN と一致します。そのため、ルール 1 がルール 2 をプリエンプション処理し、ルール 2 での VLAN 2 の照合は行われません。

```
Rule 1: allow Source Network 10.4.0.0/16
Rule 2: allow Source Network 10.4.0.0/16, VLAN 2
```

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。次に例を示します。

```
Rule 1: allow VLAN 1 URL www.example.com
Rule 2: allow VLAN 1 URL www.example.com
```

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。次に例を示します。

```
Rule 1: allow VLAN 1 URL www.example.com
Rule 2: allow VLAN 2 URL www.example.com
```

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。

- URL フィルタリングを実行するルールは、URL Filtering ライセンスがないデバイスを対象とするまで有効になっている可能性があります。その時点で、ルールの横にエラーアイコンが表示され、ポリシーをそのデバイスに適用できなくなります。適用可能にするには、このルールを編集または削除するか、ポリシーのターゲットを変更するか、または適切なライセンスを有効にする必要があります。
- 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、ルールは無効になり、その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、その後 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、そのルールは影響を与えなくなります。

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(Any)

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。モナルールを除き、トラフィックが一致する最初のルールがそのトラフィックを処理するルールになります。

アクセスコントロールルールを適切に順序付けることで、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。ユーザが作成するルールはすべての組織と展開に固有のものでありますが、ユーザ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。

重要性が最も高いルールから最も低いルールへの順序付け

最初に、組織のニーズに適するルールを順序付けする必要があります。すべてのトラフィックに適用する必要がある優先順位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、その順序に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

特定のルール、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様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できるという理由から重要です。

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、特定の他のサイトへのアクセスを許可するシナリオを想定してください。たとえば、グラフィックデザイナーに対してCreative Commons FlickrやdeviantARTコンテンツへのアクセスは許可したいが、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や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。2番目のルールに照合されるトラフィックがないため、利用可能にしようとしたコンテンツにグラフィック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

検出、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。信頼ルールやブロックルールは、システムが別の方法で検査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ます。他の要素がすべて同等である、つまりルールのセットで、より重要というルールがなく、プリエンプションが問題ではない場合には、次の順序でルールを配置することを考慮してください。

- 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(Any)

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の調査目的に使用できます。


表 12-8 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
ポリシー情報	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。
デバイス ターゲット (Device Targets)	ポリシーがターゲットとする管理対象デバイスがリストされます。
HTTP ブロック レスポンス (HTTP Block Response) HTTP インタラクティブ ブロック レスポンス (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示されます。
セキュリティ インテリジェンス (Security Intelligence)	ポリシーのセキュリティ インテリジェンスのホワイトリストおよびブラックリストの詳細が示されます。
デフォルト アクション (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。
ルール (Rule)	ポリシーの各アクセスコントロールルールが示され、その設定の詳細が示されます。
詳細設定 (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応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
参照オブジェクト (Referenced Objects)	侵入ポリシーの変数セットや 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を提供します。

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の比較\(12-31 ページ\)](#)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:

アクセス:Admin/Access Admin/Network Admin

-
- 手順 1** [ポリシー(Policies)] > [アクセス制御(Access Control)] を選択します。
[アクセスコントロールポリシー(Access Control Policy)] ページが表示されます。
- 手順 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。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。
-

アクセスコントロールポリシーの比較

ライセンス:任意(Any)

組織の標準に準拠していることを確認するためや、システム パフォーマンスを最適化するために、ポリシーの変更を検討する際には、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、[実行中の設定(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。

- [アクセスコントロールポリシー比較ビューの使用\(12-31 ページ\)](#)
- [アクセスコントロールポリシー比較レポートの使用\(12-32 ページ\)](#)

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(Any)

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と特定されます。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つのポリシー間の差異は、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 12-9 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	タイトルバーの上にある [前へ(Previous)] または [次へ(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、表示している違いを示す [差異(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	[新しい比較(New Comparison)] をクリックします。 [比較の選択(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(12-32 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	[比較レポート(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(Any)

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差異(2つのアクセスコントロールポリシーの差異、またはあるポリシーと現在適用中のポリシーとの差異)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は、[表 12-8\(12-30 ページ\)](#)に記載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 ポリシー、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、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つのアクセスコントロールポリシーを比較する方法:

アクセス:Admin/Access Admin/Network Admin

- 手順 1 [ポリシー(Policies)] > [アクセス制御(Access Control)] を選択します。
[アクセスコントロールポリシー(Access Control Policy)] ページが表示されます。
- 手順 2 [ポリシーの比較(Compare Policies)] をクリックします。

[比較の選択 (Select Comparison)] ウィンドウが表示されます。

- 手順 3** [比較対象 (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、[他のポリシー (Other Policy)] を選択します。
ページが更新されて、[ポリシー A (Policy A)] と [ポリシー B (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。
 - 現在のアクティブ ポリシーを他のポリシーに対して比較するには、[実行中の設定 (Running Configuration)] を選択します。
ページが更新されて、[ターゲット/実行中の設定 A (Target/Running Configuration A)] と [ポリシー B (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。
- 手順 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は、[ポリシー A (Policy A)] と [ポリシー B (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、[ポリシー B (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。
- 手順 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。
- 手順 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 [比較レポート (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。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。
-

