Attack Response Controller でのブロッキングとレート制限の設定

ブロックまたはレート制限を実装して攻撃を制御するようにIPSデバイスを設定できます。ブロッキングとレート制限は、主に無差別モードで動作している場合に使用します。インラインモードで動作している場合は、IPS でトラフィックをドロップする方がはるかに効率的です。ブロッキングとレート制限は、IPS の要求時に他のデバイスが実装するアクションです。このため、ブロッキングとレート制限の設定は、単純なインライン拒否よりも複雑な設定になります。

ブロッキングまたはレート制限を設定するには、ブロッキングを実行するネットワークデバイスを特定する必要があります。ブロッキングを実行するネットワークデバイスは、ブロッキングデバイスと呼ばれます。ブロッキングをサポートするために、Cisco IOS ルータおよびCatalyst 6500 スイッチ、Cisco セキュリティ アプライアンス（ASA、PIX、および FWSM）、Catalyst オペレーティング システムを実行しているCatalyst 6500/7600 デバイスなど、多くのネットワークデバイスを使用できます。別のIPSデバイスをメインブロッキングセンサーとして動作するように設定することもできます。

IPS ブロッキングについて

IPS の Attack Response Controller（ARC）コンポーネントは、攻撃しているホストとネットワークからのアクセスをブロックすることで、疑わしいイベントに対してネットワークデバイスを管理します。ARC は、管理しているデバイスの IP アドレスをブロックします。他のメインブロッキングセンサーを含め、管理しているすべてのデバイスに同じブロックを送信します。ARC は、ブロックの時間をモニタし、時間の経過後にブロックを削除します。

（注） ARC は、以前は Network Access Controller と呼ばれていました。名前は変更されましたが、IPS のマニュアルおよび設定インターフェイスでは、Network Access Controller、nac、および network-access という名前で呼ばれています。

ARCは、7秒以内に新しいブロックのアクション応答を完了します。ほとんどの場合は、より短い時間でアクション応答を完了します。このパフォーマンス目標を達成するために、センサーでのブロックの実行レートが高すぎたり、管理するブロッキングデバイスおよびインターフェイスが多すぎたりしないように設定してください。最大ブロック数は250以下にし、最大ブロッキング項目数は 10 以下にすることを推奨します。ブロッキング項目の最大数を計算するために、セキュリティ アプライアンスはブロッキング コンテキストあたり 1 つのブロッキング項目としてカウントします。ルータは、ブロッキング インターフェイス/方向あたり 1 つのブロッキング項目としてカウントします。Catalyst ソフトウェアを実行しているスイッチは、ブロッキング VLAN あたり 1 つのブロッキング項目としてカウントします。推奨される制限を超えた場合、ARC はブロックをタイミングよく適用しなかったり、ブロックをまったく適用できなかったりすることがあります。

マルチ コンテキスト モードで設定されているセキュリティ アプライアンスでは、Cisco IPS は VLAN 情報をブロック要求に含めません。したがって、ブロックされる IP アドレスが各セキュリティ アプライアンスに対して正しいことを確認する必要があります。たとえば、センサーは、VLAN A に対して設定されているセキュリティ アプライアンス カスタマー コンテキストでパケットをモニタリングする一方で、VLAN B に対して設定されている別のセキュリティ アプライアンス カスタマー コンテキストでブロッキングしている場合があります。VLAN A でブロックをトリガーするアドレスは、VLAN B 上の別のホストを参照します。

（注） ブロッキングは、マルチ コンテキスト モードの管理コンテキストでは FWSM でサポートされません。

ブロックには次の 3 種類があります。

- ホスト ブロック：特定の IP アドレスからのすべてのトラフィックをブロックします。

シグニチャがトリガーされたときに自動ホストブロックを開始するように IPS を設定するには、[ホストのブロックを要求（Request Block Host）] イベントアクションをシグニチャに追加するか、イベント アクション オーバーライド ポリシーを使用してリスクレーティングに基づくイベントに追加します。イベント アクション オーバーライドの設定およびシグニチャの設定を参照してください。

- 接続ブロック：特定の送信元 IP アドレスから特定の宛先 IP アドレスおよび宛先ポートへのトラフィックをブロックします。同じ送信元 IP アドレスから異なる宛先 IP アドレスまたは宛先ポートへの複数の接続ブロックによって、接続ブロックからホストブロックにブロックが自動的に切り替えられます。

シグニチャがトリガーされたときに自動接続ブロックを開始するように IPS を設定するには、[接続のブロックを要求（Request Block Connection）] イベントアクションをシグニチャに追加

するか、イベント アクション オーバーライド ポリシーを使用してリスクレーティングに基づくイベントに追加します。

- ネットワーク ブロック：特定のネットワークからのトラフィックをすべてブロックします。

ホストブロックと接続ブロックは、手動で開始するか、シグニチャがトリガーされたときに自動的に開始できます。ネットワーク ブロックは手動でだけ開始できます。ネットワークブロックは Security Manager から開始できません。代わりに IPS Device Manager を使用します。

ヒント 接続ブロックとネットワーク ブロックは、セキュリティ アプライアンス（ファイアウォール）ではサポートされません。セキュリティ アプライアンスでは、追加の接続情報があるホストブロックだけがサポートされます。

（注） ブロッキングとセンサーのパケット ドロップ機能を混同しないでください。センサーでは、インライン モードのセンサーに対してパケットのインライン拒否、接続のインライン拒否、および攻撃者のインライン拒否のアクションが設定されている場合にパケットをドロップできます。

Cisco IOS ソフトウェア デバイス（ルータおよび Catalyst 6500 シリーズ スイッチ）では、ARC は、ACL を適用することでブロックを作成します。Catalyst オペレーティング システムを実行する Catalyst 6500/7600 デバイスでは、ARC は VACL を適用することでブロックを作成します。ACL および VACL は、インターフェイス方向または VLAN 上のデータ パケットの経路を許可または拒否します。各 ACL または VACL には、IP アドレスに適用される許可条件と拒否条件が含まれます。セキュリティアプライアンスでは、**shun** コマンドが ACL の代わりに使用されます。

ヒント ブロッキングデバイスとして設定できる特定のデバイスおよびオペレーティング システム バージョンのリストについては、使用している IPS ソフトウェアバージョンの『*Installing and Using Cisco Intrusion Prevention System Device Manager*』の「Configuring Attack Response Controller for Blocking and Rate Limiting」の章で、サポートされるデバイス情報を参照してください。これらの資料は、Cisco.com の http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_installation_and_configuration_guides_list.html [英語] から入手できます。

次の各項で、IPS ブロッキングについて詳細に説明します。

- ブロック適用のストラテジ （4 ページ）
- レート制限について （5 ページ）
- ルータおよびスイッチ ブロッキング デバイスについて （5 ページ）

- メインブロッキングセンサーについて （7 ページ）
- IPS のブロッキングおよびレート制限の設定 （8 ページ）
- [Blocking] ページ （11 ページ）

ブロック適用のストラテジ

ブロッキングは、イベントの発生時に、イベントに [Request Block Connection] または [Request Block Host] イベント アクションが含まれる場合にだけ実行されます。これらのイベント アクションは、通常、拒否アクションを使用して不要なトラフィックをドロップするインライン モードで IPS を操作している場合には不要です。

ブロッキング アクションの実装が必要になる状況は次のとおりです。

- 無差別モード：無差別モードで実行している場合、IPS は拒否アクションを実装できません。このため、ホストからのトラフィックを防ぐには、ブロッキングを実装する必要があります。
- インラインモード：インラインモードでは、拒否アクションを実装して不要なトラフィックを即時にドロップできます。ただし、ネットワークの他のセグメントを保護するためにブロッキング アクションの追加が必要な場合があります。

たとえば、ネットワークが A、B、C、D、E の 5 つのサブネットから構成され、これらの各セグメントに、それをモニタしているインライン IPS デバイスがあるとします。サブネット A の IPS が攻撃を識別した場合、IPS は拒否アクションを使用してサブネット A を保護できるだけでなく、ブロック要求アクションを使用して B、C、D、E を保護するファイアウォールを設定し、攻撃がこれらの他のサブネットをターゲットとする前に攻撃者を避けることもできます。この例では、1 つの IPS をメインブロッキングセンサーとして指定し、他の 4 つの IPS センサーで、メインブロッキングセンサーを介したブロッキングを実行させます。

次の手法を使用して、ブロック要求アクションをイベントに追加します。

- イベント アクション オーバーライド ポリシー：イベント アクション オーバーライド ルールを設定して、イベントのリスク レーティングに基づいてすべてのイベントにアクションを追加します。これは単純なアプローチです。拒否アクションの追加に使用されるのと同じリスク レーティングでブロック要求アクションを追加できます。詳細については、イベント アクション オーバーライドの設定を参照してください。
- シグニチャ ポリシー：ブロック要求アクションを個々のシグニチャに追加できます。これには、各シグニチャを編集してアクションを追加する必要があります。これは時間のかかるアプローチとなる場合がありますが、最も関心のあるイベント タイプだけにブロッキングを設定できます。詳細については、シグニチャの設定を参照してください。

関連項目

- IPS ブロッキングについて （1 ページ）
- メインブロッキングセンサーについて （7 ページ）

• インターフェイス モードについて
• IPS のブロッキングおよびレート制限の設定 （8 ページ）
• [Blocking] ページ （11 ページ）

レート制限について

Attack Response Controller（ARC）は、保護されているネットワーク内のトラフィックのレート制限を行います。レート制限により、センサーはネットワークデバイス上の指定したトラフィック クラスのレートを制限できます。レート制限応答は、Host Flood エンジンと Net Flood エンジン、および TCP ハーフオープン SYN シグニチャに対してサポートされます。ARC では、Cisco IOS 12.3 以降を実行しているネットワーク デバイスにレート制限を設定できます。メインブロッキングセンサーは、レート制限要求をブロッキング転送センサーに転送することもできます。

シグニチャにレート制限を追加するには、[Request Rate Limit] アクションを追加する必要があります。次に、シグニチャ パラメータを編集して、Event Actions Settings フォルダにこれらのシグニチャのパーセンテージを設定します。

ヒント レート制限は手動でも実装できますが、Security Manager を使用した実装はできません。代わりに IPS Device Manager を使用します。

ブロッキング デバイスでは、レート制限が設定されているインターフェイス/方向にサービス ポリシーを適用しないでください。適用した場合は、レート制限アクションが失敗します。レート制限を設定する前に、インターフェイス/方向にサービス ポリシーがないことを確認し、存在する場合には削除します。ARC では、ARC が以前に追加したものでないかぎり、既存のレート制限は削除されません。

レート制限では ACL が使用されますが、ブロックと同じ方法では使用されません。レート制限では、ACL および class-map エントリを使用してトラフィックを識別し、policy-map および service-policy エントリを使用してトラフィックをポリシングします。

ルータおよびスイッチ ブロッキング デバイスについて

Cisco IOS ソフトウェアを実行しているルータまたは Catalyst 6500/7600 デバイス、あるいは Catalyst オペレーティング システムを実行している Catalyst 6500/7600 デバイスを使用して、ネットワークに IPS ブロッキングを実装できます。ルータまたはスイッチを使用する場合、Attack Response Controller（ARC）では、拡張 ACL（IOS デバイス上）または VLAN ACL（Catalyst OS デバイス上）を設定してブロックが実装されます。これらの ACL と VACL は、同じ方法で作成および管理されます。

レート制限でも ACL が使用されますが、ブロックと同じ方法では使用されません。レート制限では、ACL および class-map エントリを使用してトラフィックを識別し、policy-map および service-policy エントリを使用してトラフィックをポリシングします。

ヒント　IPS は、Cisco IOS ソフトウェアを実行している Catalyst 6500/7600 デバイスをルータと同等と見なします。これらのデバイスをブロッキングデバイスとして追加する場合は、ルータとして追加します。

ルータ インターフェイスまたはスイッチ VLAN をブロッキング インターフェイスとして設定する場合は、オプションで、pre-ACL/VACL および post-ACL/VACL の名前を指定できます。ACL 名または VACL 名の指定は任意ですが、インターフェイスまたは VLAN に ACL または VACL を設定した場合は、それらも IPS に対して指定する必要があります。そうしないと、その ACL または VACL は ARC によってデバイス設定から削除されます。

pre-ACL/VACL および post-ACL/VACL には次の用途があります。

- Pre-Block ACL/VACL は、主にセンサーでブロックしない対象を許可する場合に使用します。パケットが ACL/VACL に対してチェックされると、最初に一致した行によってアクションが決定されます。最初の行が Pre-Block ACL/VACL の permit 行と一致する場合、パケットは、ACL/VACL であとに（自動ブロックからの）deny 行がある場合でも許可されます。Pre-Block ACL/VACL では、ブロックの結果の deny 行をオーバーライドできます。
- Post-Block ACL/VACL は、同じインターフェイスまたは方向で追加のブロッキングまたは許可を行う場合に最もよく使用されます。センサーが管理するインターフェイスまたは方向に既存の ACL がある場合は、その既存の ACL を Post-Block ACL/VACL として使用できます。Post-Block ACL/VACL がない場合、センサーは新しい ACL/VACL の最後に permit ip any any を挿入します。

IOS ソフトウェア ブロッキング デバイスを Security Manager で管理している場合は、ブロッキングデバイスを選択し、[ツール（Tools）]>[設定のプレビュー（Preview Config）] を選択することで ACL 名を識別できます。インターフェイス設定で **ip access-group** コマンドを検索し、方向を確認します。たとえば、次の行は、CSM_FW_ACL_GigabitEthernet0/1 という名前の ACL が、GigabitEthernet0/1 インターフェイスに接続された In 方向に存在することを示しています。

```
interface GigabitEthernet0/1
  ip access-group CSM_FW_ACL_GigabitEthernet0/1 in
```

この例では、ブロッキング インターフェイスとして GigabitEthernet0/1 を In 方向に設定する場合、pre-ACL または post-ACL として、CSM_FW_ACL_GigabitEthernet0/1 を必ず指定してください。ほとんどの場合は、ACL を post-ACL として指定します。これにより、比較的短い IPS ブロッキング ACL によって望ましくないトラフィックが最初に除外され、その後、ブロッキング デバイスによって他のアクセス ルールが実行されます。

Security Manager では Catalyst OS デバイスが管理されないため、VACL 名を判断するには Security Manager の外部で Catalyst OS デバイス設定を調べる必要があります。IOS ソフトウェアを実行する Catalyst 6500/7600 デバイスにも VACL がある場合がありますが、デバイスが IOS ソフトウェアを実行している場合、IPS は Catalyst 6500/7600 VLAN で VLAN ブロッキングを実行しないことに注意してください。

センサーは、起動時に 2 つの ACL/VACL の内容を読み取ります。センサーは次のエントリをこの順序で持つ第 3 の ACL/VACL を作成し、この結合された ACL/VACL がインターフェイスまたは VLAN に適用されます。

1. センサー IP アドレス、またはセンサーの NAT アドレス（指定されている場合）がある **permit** 行

[Blocking] ポリシーの [General] タブで [Allow Sensor IP address to be Blocked] オプションを選択した場合、この permit エントリは追加されません。詳細については、[General] タブ、IPS ブロッキング ポリシー （14 ページ）を参照してください。

1. Pre-Block ACL/VACL（指定されている場合）。
2. IPS によって生成された任意のアクティブ ブロック（deny ステートメント）。
3. Post-Block ACL/VACL（指定されている場合）。

Post-Block ACL/VACL を指定しない場合は、すべてのフィルタされないトラフィックを許可するために **permit ip any any** エントリが追加されます。これにより、インターフェイス ACL を終了する通常の暗黙の deny any が否定されます。

Catalyst OS を使用している場合、IDSM-2 は新しい VACL の最後に **permit ip any any capture** を挿入します。

ARC がデバイスを管理し、そのデバイスで ACL/VACL を設定する必要がある場合は、最初にブロッキングをディセーブルにする必要があります。ユーザと ARC の両方が同じデバイスで同時に変更を加える状況を回避する必要があります。この状況が発生すると、デバイスまたは ARC でエラーが発生します。Pre-Block ACL/VACL または Post-Block ACL/VACL を修正する必要がある場合は、次の手順に従います。

1. センサーでブロッキングをディセーブルにします。

一時的な変更を加えるため、デバイスで IPS Device Manager（IDM）を使用して、ブロッキングをディセーブルにし、再びイネーブルにできます。または、Security Manager の [Blocking] ポリシーの [General] タブで [Enable Blocking] オプションを選択解除してから、IPS センサーに設定を展開できます。ブロッキングを再びイネーブルにするには、[Enable Blocking] オプションをもう一度選択し、IPS センサーに設定を展開します。

1. デバイスの設定に変更を加えます。たとえば、Security Manager でブロッキング デバイスを管理する場合は、更新した設定を展開し、デバイスがリロードされるまで待ちます。
2. センサーでブロッキングを再びイネーブルにします。

メインブロッキングセンサーについて

複数のセンサー（ブロッキング転送センサー）が、1 つ以上のデバイスを制御する、指定したメインブロッキングセンサーに、ブロッキング要求を転送できます。メインブロッキングセンサーは、他の 1 つ以上のセンサーに代わって 1 つ以上のデバイスでブロッキングを制御するセンサーで実行されている ARC です。ブロッキングまたはレート制限要求がイベントアクショ

ンとして設定されているシグニチャが出現した場合、センサーはブロック要求またはレート制限要求をメインブロッキングセンサーに転送し、そのセンサーがブロックまたはレート制限を実行します。

メインブロッキングセンサーを追加する場合は、センサーあたりのブロッキングデバイス数を減らします。たとえば、それぞれ 1 つのブロッキング インターフェイス/方向を持つ 10 個のファイアウォールと 10 台のルータでブロックする場合は、センサーに 10 個を割り当て、メインブロッキングセンサーに残りの 10 個を割り当てることができます。

[Blocking] ページ （11 ページ）の説明に従って、[ブロッキング（Blocking）] ポリシーの [プライマリブロッキングセンサー（Primary Blocking Sensors）] タブで、メインブロッキングセンサーを設定します。

メインブロッキングセンサーを設定する場合は、次のヒントを考慮してください。

- 2 つのセンサーが同じデバイスでブロッキングまたはレート制限を制御することはできません。この状況が必要な場合は、一方のセンサーをメインブロッキングセンサーとして設定してデバイスを管理し、もう一方のセンサーでメインブロッキングセンサーに要求を転送できます。
- ブロッキング転送センサーで、マスターブロッキングセンサーとして機能するリモートホストを識別します。メインブロッキングセンサーでは、[許可ホスト（Allowed Hosts）] ポリシーを使用してアクセスリストにブロッキング転送センサーを追加する必要があります。許可ホストの識別を参照してください。
- メインブロッキングセンサーが Web 接続に TLS を必要とする場合は、メイン ブロッキングセンサー リモート ホストの X.509 証明書を受け入れるようにブロッキング転送センサーの ARC を設定する必要があります。センサーでは TLS がデフォルトでイネーブルになりますが、このオプションは変更できます。詳細については、[プライマリブロッキングセンサー（Primary Blocking Sensors）] ダイアログボックス （17 ページ） を参照してください。
- 通常、メインブロッキングセンサーはネットワークデバイスを管理するように設定します。ブロッキング転送センサーは、通常は他のネットワーク デバイスを管理するようには設定されていませんが、これを行うことは可能です。
- 1 つのセンサーだけがデバイス上のすべてのブロッキング インターフェイスを制御する必要があります。

IPS のブロッキングおよびレート制限の設定

任意のシグニチャで [Request Block Host]、[Request Block Connection]、または [Request Rate Limit] アクションを使用する場合、またはイベント アクション オーバーライド ポリシーを使用してこれらのアクションをイベントに追加する場合は、ブロッキング デバイスを設定する必要があります。これらのアクションを使用しない場合は、ブロッキング デバイスを設定する必要はありません。

ブロッキングを設定する前に、次の各項を参照してください。

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから[プラットフォーム（Platform）]>[セキュリティ（Security）] > [ブロッキング（Blocking）] を選択します。
- （ポリシー ビュー）[IPS] > [プラットフォーム（Platform）] > [セキュリティ（Security）] > [ブロッキング（Blocking）] を選択してから、既存のポリシーを選択するか、新しいポリシーを作成します。

ブロッキング ポリシーの概要については、 [Blocking] ページ （11 ページ）を参照してください。

ステップ 2 [General] タブで、デフォルト以外の値が必要な設定を変更します。ただし、デフォルト値はほとんどのネットワークに適しています。設定の詳細については、 [General] タブ、IPS ブロッキング ポリシー （14 ページ） を参照してください。

ステップ 3 [ユーザプロファイル（User Profiles）] タブをクリックし、ブロッキングデバイスへのログインに必要なユーザプロファイルを作成します。

- プロファイルを追加するには、[行の追加（Add Row）] ボタンをクリックし、[ユーザープロファイルの追加（Add User Profile）] ダイアログボックスに入力します（ [Add User Profile]/[Modify User Profile] ダイアログボックス （17 ページ）を参照）。
- プロファイルを編集するには、プロファイルを選択し、[行の編集（Edit Row）] ボタンをクリックします。
- プロファイルを削除するには、プロファイルを選択し、[行の削除（Delete Row）] ボタンをクリックします。プロファイルを削除する前に、ブロッキング デバイスによって現在使用されていないことを確認してください。

ステップ 4 メインブロッキングセンサーについて （7 ページ）で説明するようにメインブロッキングセンサーを使用する必要がある場合は、[プライマリブロッキングセンサー（Primary Blocking Sensors）] タブをクリックし、次の操作を行います。

- メインブロッキングセンサーを追加するには、[行の追加（Add Row）] ボタンをクリックし、[メインブロッキングセンサーの追加（Add Main Blocking Sensor）] ダイアログボックスに入力します（[プライマリブロッキングセンサー（Primary Blocking Sensors）] ダイアログボックス （17 ページ）を参照）。
- メインブロッキングセンサーを編集するには、メインブロッキングセンサーを選択し、[行の編集（Edit Row）] ボタンをクリックします。

- メインブロッキングセンサーを削除するには、メインブロッキングセンサーを選択し、[行の削除（Delete Row）] ボタンをクリックします。

ステップ 5 （メインブロッキングセンサーだけを使用するのでないかぎり）ブロッキングデバイスを指定します。デバイスを適切なタブに追加する必要があります。

- [ルータ（Routers）] タブ：IOS ソフトウェアを実行している Catalyst 6500 スイッチを含むすべての Cisco IOS ソフトウェアデバイスの場合。
- [ファイアウォールFirewalls] タブ：ASA、PIX、および FWSM の場合。
- [Catalyst 6K] タブ：Catalyst オペレーティングシステムを実行している Catalyst 6500/7600 デバイスの場合。

各タブでの設定手順は同じです。

- デバイスを追加するには、[行の追加（Add Row]） ボタンをクリックし、[ルータデバイスの追加（Add Router Device）]/[ファイアウォールデバイスの追加（Add Firewall Device）]/[Cat6Kデバイスの追加（Add Cat6K Device）] ダイアログボックスに入力します（[Add Router Device]/[Modify Router Device]、[Add Firewall Device]/[Modify Firewall Device]、[Add Cat6K Device]/[Modify Cat6K Device] ダイアログボックス （19 ページ）を参照）。
- デバイスを編集するには、そのデバイスを選択して [行の編集（Edit Row）] ボタンをクリックします。
- デバイスを削除するには、そのデバイスを選択して [行の削除（Delete Row）] ボタンをクリックします。

ステップ 6 [ブロックしないホスト（Never Block Hosts）]/[ブロックしないネットワーク（Never Block Networks）] タブをクリックし、ブロックしないホストとネットワークを指定します。これらのリストはブロッキングアクションに影響しますが、制限アクションには影響しません。信頼できるネットワークとホストを識別します。

- ホストまたはネットワークを追加するには、該当するテーブルの下にある [行の追加（Add Row）] ボタンをクリックし、[ブロックしないホストの追加（Add Never Block Host）]/[ブロックしないネットワークの追加（Add Never Block Network）] ダイアログボックスに入力します（[Add Never Block Host]/[Modify Never Block Host] または [Add Never Block Network]/[Modify Never Block Network] ダイアログボックス （23 ページ）を参照）。
- ホストまたはネットワークを編集するには、ホストまたはネットワークを選択し、[行の編集（Edit Row）] ボタンをクリックします。
- ホストまたはネットワークを削除するには、ホストまたはネットワークを選択し、[行の削除（Delete Row）] ボタンをクリックします。

[Blocking] ページ

[Blocking] ページを使用して、IPS センサーのブロッキング プロパティを設定します。シグニチャまたはイベント アクション ポリシーで [Request Block Connection]、[Request Block Host]、または [Request Rate Limit] のイベント アクションを使用する場合にだけ、ブロッキング ポリシーを設定します。ブロッキング ホストは、これらのアクションが割り当てられているイベントにだけ使用されます。

ヒント ブロックしないホストとネットワークのリストは、[Request Block Connection] および [Request Block Host] イベント アクションにだけ適用されます。リストはレート制限には影響せず、[Deny Packet Inline] などの拒否アクションにも影響しません。ホストとネットワークを拒否アクションまたはレート制限アクションから免除するには、イベント アクション フィルタ ルールを使用し、ホストとネットワークを攻撃者として指定し、イベントからアクションを削除します。詳細については、イベント アクション フィルタの設定を参照してください。

ナビゲーション パス

- （デバイス ビュー）ポリシー セレクタから [プラットフォーム（Platform）] > [セキュリティ（Security）] > [ブロッキング（Blocking）] を選択します。
- （ポリシー ビュー）[IPS] > [プラットフォーム（Platform）] > [セキュリティ（Security）] > [ブロッキング（Blocking）] を選択してから、既存のポリシーを選択するか、新しいポリシーを作成します。

関連項目

- IPS のブロッキングおよびレート制限の設定 （8 ページ）
- IPS ブロッキングについて （1 ページ）
- ブロック適用のストラテジ （4 ページ）
- レート制限について （5 ページ）
- ルータおよびスイッチ ブロッキング デバイスについて （5 ページ）
- メインブロッキングセンサーについて （7 ページ）
- IPS イベント アクションについて

フィールド リファレンス

表 *1 : IPS* ブロッキング ポリシー

要素	説明
[一般（General）] タブ	ブロッキングとレート制限をイネーブルにするために必要な基本設定。[General] タブのオプションの詳細については、[General] タブ、IPS ブロッキング ポリシー （14 ページ）を参照してください。
[User Profiles] タブ	ブロッキングデバイスにログインするための接続クレデンシャル情報プロファイル。ブロッキング デバイスを定義する前に、デバイスへのログインに必要なユーザ プロファイルを作成します。この表には、プロファイル名、ユーザ名、および固定数のアスタリスクでマスクされたパスワードが表示されます。 • プロファイルを追加するには、[行の追加（Add Row）] ボタンをクリックし、[ユーザープロファイルの追加（Add User Profile）] ダイアログボックスに入力します（[Add User Profile]/[Modify User Profile] ダイアログボックス （17 ページ）を参照）。 • プロファイルを編集するには、プロファイルを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • プロファイルを削除するには、プロファイルを選択し、[行の削除（Delete Row）] ボタンをクリックします。プロファイルを削除する前に、ブロッキングデバイスによって現在使用されていないことを確認してください。
[プライマリ ブロッキング センサー（Primary Blocking Sensors）] タブ	メインブロッキング IPS センサー（メインブロッキングセンサーについて （7 ページ）を参照）。メインブロッキングセンサーは、他の IPS デバイスのブロックを管理します。このテーブルには、メインブロッキングセンサーの IP アドレス（またはネットワーク/ホストオブジェクト）、そのセンサーにログインするためのユーザー名とパスワード、接続に使用するポート、およびログインに TLS が使用されるかどうかが表示されます。 • メインブロッキングセンサーを追加するには、[行の追加（Add Row）] ボタンをクリックし、[プライマリブロッキングセンサーの追加（Add Master Blocking Sensor）] ダイアログボックスに入力します（メインブロッキングセンサーについて （7 ページ）を参照）。 • メインブロッキングセンサーを編集するには、メインブロッキングセンサーを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • メインブロッキングセンサーを削除するには、メインブロッキングセンサーを選択し、[行の削除（Delete Row）] ボタンをクリックします。

要素	説明
[Router] タブ	ブロッキング デバイスまたはレート制限デバイスとして使用する IOS ルータと（IOS ソフトウェアを実行している）Catalyst 6500/7600 デバイス。このテーブルに、デバイスの IP アドレス（またはネットワーク/ホスト オブジェクト）、デバイスへのログインに使用する通信方法、センサーの NAT アドレス（NAT が使用されない場合は 0.0.0.0）、デバイスへのログインに使用するプロファイルの名前、およびデバイスの応答機能（ブロッキング、レート制限、またはその両方）が表示されます。 • ルータを追加するには、[行の追加（Add Row）] ボタンをクリックし、[ルータデバイスの追加（Add Router Device）] ダイアログボックスに入力します（[プライマリブロッキングセンサー（Primary Blocking Sensors）] ダイアログボックス （17 ページ）を参照）。 • ルータを編集するには、ルータを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • ルータを削除するには、ルータを選択し、[行の削除（Delete Row）] ボタンをクリックします。
[Firewall] タブ	ブロッキング デバイスとして使用する ASA、PIX、および FWSM デバイス。この表に、デバイスの IP アドレス（またはネットワーク/ホスト オブジェクト）、デバイスへのログインに使用する通信方法、センサーの NAT アドレス（NAT が使用されない場合は 0.0.0.0）、デバイスへのログインに使用するプロファイルの名前を示します。 • ファイアウォールを追加するには、[行の追加（Add Row）] ボタンをクリックし、[ファイアウォールデバイスの追加（Add Firewall Device）] ダイアログボックスに入力します（ [Add Router Device]/[Modify Router Device]、[Add Firewall Device]/[Modify Firewall Device]、[Add Cat6K Device]/[Modify Cat6K Device] ダイアログボックス （19 ページ）を参照）。 • ファイアウォールを編集するには、ファイアウォールを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • ファイアウォールを削除するには、ファイアウォールを選択し、[行の削除（Delete Row）] ボタンをクリックします。

要素	説明
[Catalyst 6K] タブ	ブロッキング デバイスとして使用する、Catalyst ソフトウェアを使用している Catalyst 6500/7600 デバイス。この表に、デバイスの IP アドレス（またはネットワーク/ホスト オブジェクト）、デバイスへのログインに使用する通信方法、センサーの NAT アドレス（NAT が使用されない場合は 0.0.0.0）、デバイスへのログインに使用するプロファイルの名前を示します。 ヒント　Cisco IOS ソフトウェアを実行している Catalyst 6500/7600 デバイスには、このタブを使用しないでください。代わりに、[Router] タブを使用します。 • Catalyst OS デバイスを追加するには、[行の追加（Add Row）] ボタンをクリックし、[Cat6Kデバイスの追加（Add Cat6K Device）] ダイアログボックスに入力します（[Add Router Device]/[Modify Router Device]、[Add Firewall Device]/[Modify Firewall Device]、[Add Cat6K Device]/[Modify Cat6K Device] ダイアログボックス （19 ページ）を参照）。 • Catalyst OS デバイスを編集するには、そのデバイスを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • Catalyst OS デバイスを削除するには、そのデバイスを選択し、[行の削除（Delete Row）] ボタンをクリックします。
[Never Block Hosts]/[Never Block Networks]	ブロックしないホストとネットワーク。ホストとネットワークは別々の表に表示されます。これらの表には、ホストまたはネットワークの IP アドレスまたはネットワーク/ホスト オブジェクトが表示されます。これらのリストは、レート制限アクションに影響せず、拒否アクションにも適用されません。 • ホストまたはネットワークを追加するには、該当するテーブルの下にある [行の追加（Add Row）] ボタンをクリックし、[ブロックしないホストの追加（Add Never Block Host）]/[ブロックしないネットワークの追加（Add Never Block Network）] ダイアログボックスに入力します（[Add Never Block Host]/[Modify Never Block Host] または [Add Never Block Network]/[Modify Never Block Network] ダイアログボックス （23 ページ）を参照）。 • ホストまたはネットワークを編集するには、ホストまたはネットワークを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • ホストまたはネットワークを削除するには、ホストまたはネットワークを選択し、[行の削除（Delete Row）] ボタンをクリックします。

[General] タブ、IPS ブロッキング ポリシー

[Blocking] ポリシーの [General] タブを使用して、ブロッキングとレート制限をイネーブルにするために必要な基本設定を設定します。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [セキュリティ（Security）] > [ブロッキング（Blocking）] を選択します。必要に応じて、[全般（General）] タブを選択します。
- （ポリシービュー）[IPS] > [プラットフォーム（Platform）] > [セキュリティ（Security）] > [ブロッキング（Blocking）] を選択してから、既存のポリシーを選択するか、新しいポリシーを作成します。必要に応じて、[全般（General）] タブを選択します。

関連項目

- IPS ブロッキングについて （1 ページ）
- IPS のブロッキングおよびレート制限の設定 （8 ページ）
- [Blocking] ページ （11 ページ）

フィールド リファレンス

表 *2 : [General]* タブ、*IPS* ブロッキング ポリシー

要素	説明
Log All Block Events and Errors	開始から終了までブロックに続くイベントおよび発生したエラー メッセージをログに記録するかどうか。ブロックがデバイスに追加されるかデバイスから削除されると、イベントがログに記録されます。これらすべてのイベントおよびエラーをログに記録する必要はない可能性があります。このオプションをディセーブルにすると、新しいイベントとエラーが抑止されます。デフォルトではイネーブルになっています。 （注） すべてのブロック イベントとエラーの記録はレート制限にも適用されます。
Enable NVRAM Write	Attack Response Controller（ARC）が最初に接続するときにルータが Non-Volatile RAM（NVRAM; 不揮発性 RAM）に書き込むようにするかどうか。イネーブルになっている場合は、ACL が更新されるたびに NVRAM が書き込まれます。デフォルトではディセーブルになっています。 NVRAM の書き込みをイネーブルにすると、ブロッキングとレート制限に対するすべての変更が NVRAM に必ず書き込まれます。ルータが再起動された場合でも、適切なブロックとレート制限がアクティブになります。NVRAM の書き込みがディセーブルになっている場合、ルータの再起動後にブロッキングまたはレート制限が行われない期間が短時間発生します。NVRAM 書き込みをイネーブルにしない場合、NVRAM の寿命が延び、新しいブロックとレート制限の設定にかかる時間が短縮されます。

要素	説明
Enable ACL Logging	ARC で、アクセス コントロール リスト（ACL）または VLAN ACL（VACL）のブロック エントリにログ パラメータを追加するかどうか。これにより、デバイスはパケットがフィルタ処理されるときに syslog イベントを生成します。このオプションは、ルータとスイッチにだけ適用されます。デフォルトではディセーブルになっています。
Allow Sensor IP address to be Blocked	センサー IP アドレスをブロックできるかどうか。デフォルトではディセーブルになっています。 **ヒント** センサー アドレスのブロックを許可した場合、IPS は、IPS アドレスを許可するために明示的な permit エントリをインターフェイス ACL に追加しません。IPS アドレスがデバイス ACL によって許可されていることを確認する必要があります。そうしないと、IPS はデバイスでブロッキングを実装できません。
Enable Blocking	ホストのブロッキングおよびレート制限をイネーブルにするかどうか。デフォルトではイネーブルになっています。 **（注）** ブロッキングをイネーブルにする場合は、レート制限もイネーブルにします。ブロッキングをディセーブルにする場合は、レート制限もディセーブルにします。これは、ARC が新しいブロックまたはレート制限の追加や既存のブロックまたはレート制限の削除を行えないことを意味します。
Max Blocks	ブロックするエントリの最大数。指定できる範囲は 1 ～ 65535 です。デフォルトは 250 です。
Max Interfaces	ブロックを実行するインターフェイスの最大数。たとえば、PIX 500 シリーズ セキュリティ アプライアンスは 1 つのインターフェイスとカウントされます。1 つのインターフェイスを持つルータは 1 つとしてカウントされますが、2 つのインターフェイスを持つルータは 2 つとしてカウントされます。インターフェイスの最大数はデバイスあたり 250 です。デフォルトは 250 です。 [Max Interfaces] を使用して、ARC が管理できるデバイスとインターフェイスの数の上限を設定します。ブロッキング デバイスの合計数（メイン ブロッキング センサーを含まない）をこの値を超える数にすることはできません。ブロッキング項目の合計数もこの値を超えることはできません。ブロッキング項目は 1 つのセキュリティ アプライアンス コンテキスト、1 つのルータ ブロッキング インターフェイス/方向、または VLAN をブロッキングしている 1 つの Catalyst ソフトウェア スイッチです。 **（注）** また、デバイスあたり 100 のインターフェイス、250 台のセキュリティ アプライアンス、250 台のルータ、250 台の Catalyst ソフトウェア スイッチ、および 100 台のメイン ブロッキング センサーは上限として固定されており、変更できません。

要素	説明
Max Rate Limits	レート制限エントリの最大数。最大レート制限は、最大ブロッキングエントリ以下である必要があります。範囲は 1 ～ 32767 です。デフォルト値は 250 です。

[Add User Profile]/[Modify User Profile] ダイアログボックス

[Add User Profile]/[Modify User Profile] ダイアログボックスを使用して、IPS ブロッキング デバイスのユーザ プロファイルを追加または修正します。プロファイルでは、IPS デバイスがログインして、IPS ブロッキングを実装するルータ、スイッチ、またはファイアウォールを設定できる IPS デバイスのユーザ名とパスワードを定義します。

プロファイル名だけを持つプロファイルを保存できますが、ユーザ名、パスワード、およびイネーブル パスワードの要件はデバイスによって決定されます。デバイスに必要な項目を指定してコンフィギュレーション モードを開始する必要があります。そうしないと、IPS はデバイスにブロッキングを設定できません。

ナビゲーション パス

[IPSブロッキング（IPS Blocking）] ポリシーで、[ユーザープロファイル（User Profiles）] タブを選択し、[行の追加（Add Row）] ボタンをクリックするか、既存のセンサーを選択して [行の編集（Edit Row）] ボタンをクリックします。ブロッキング ポリシーを開く方法については、[Blocking] ページ （11 ページ）を参照してください。

フィールド リファレンス

表 3 : [Add User Profile]/[Modify User Profile] ダイアログボックス

要素	説明
プロファイル名（Profile Name）	最大 64 文字の英数字のプロファイル名。
ユーザー名	ブロッキング デバイスにログインするときに使用するユーザ名。
パスワード	ユーザ名のログイン パスワード（必要な場合）。
パスワードを有効にする（Enable Password）	特権 EXEC モード（イネーブル モード）を開始するためのイネーブル パスワード（必要な場合）。

[プライマリブロッキングセンサー（Primary Blocking Sensors）]ダイアログボックス

[プライマリブロッキングセンサーの追加（Add Primary Blocking Sensor）]/[プライマリブロッキングセンサーの変更（Modify Primary Blocking Sensor）] ダイアログボックスを使用して、メ

インブロッキングセンサーを設定します。メインブロッキングセンサーの詳細については、メインブロッキングセンサーについて （7 ページ）を参照してください。

ナビゲーション パス

[IPSブロッキング（IPS Blocking）] ポリシーで、[マスターブロッキングセンサー（Master Blocking Sensors）] タブを選択し、[行の追加（Add Row）] ボタンをクリックするか、既存のセンサーを選択して [行の編集（Edit Row）] ボタンをクリックします。ブロッキング ポリシーを開く方法については、[Blocking] ページ （11 ページ）を参照してください。

フィールド リファレンス

表 *4 : [プライマリブロッキングセンサー（Primary Blocking Sensors）] ダイアログボックス*

要素	説明
IPアドレス	メインブロッキングセンサーの IP アドレス。単一のホストアドレスが含まれたネットワーク/ホストポリシーオブジェクトの IP アドレスまたは名前を入力するか、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成します。
ユーザー名	メインブロッキングセンサーへのログインに使用するユーザー名。ユーザーアカウントは、メインブロッキングセンサーに設定されているアクティブなアカウントである必要があります。
パスワード	ユーザ名のログイン パスワード。
[ポート（Port）]	メインブロッキングセンサー上の接続先ポート。デフォルトは 443 です。
TLS	TLS を使用するかどうか。 [TLS] オプションを選択した場合は、メイン ブロッキング センサー リモート ホストの TLS/SSL X.509 証明書を受け入れるようにブロッキング転送センサーの ARC を設定する必要があります（ブロッキング転送センサーは、このブロッキング ポリシーを割り当てている任意のデバイスです）。 ブロッキング転送センサーが X.509 証明書を受け入れるように設定する最も簡単な方法は、IPS Device Manager（IDM）を使用してセンサーにログインし、[設定（Configuration）] > [センサー管理（Sensor Management）] > [証明書（Certificates）] > [信頼できるホスト（Trusted Hosts）] > [信頼できるホストの追加（Add Trusted Host）] を選択して、メインブロッキングセンサーを信頼できるホストとして追加することです。または、センサー CLI にログインし、コンフィギュレーション モードを開始して、**tls trusted-host ip-address** コマンドを使用することもできます。

[Add Router Device]/[Modify Router Device]、[Add Firewall Device]/[Modify Firewall Device]、[Add Cat6K Device]/[Modify Cat6K Device] ダイアログボックス

[Add Router Device]/[Modify Router Device]、[Add Firewall Device]/[Modify Firewall Device]、または [Add Cat6K Device]/[Modify Cat6K Device] ダイアログボックスを使用して、デバイスを IPS センサーのブロッキングデバイスとして設定します。ダイアログボックスの名前は、追加するデバイスのタイプを示します。

- [Router]：IOS ソフトウェア ルータと Catalyst 6500/7600 デバイス。これらのデバイスは、レート制限とブロッキングを実行できます。ルータおよびスイッチ ブロッキング デバイスについて （5 ページ）を参照してください。
- [Firewall]：ASA および PIX アプライアンス。
- [Cat6K]：Catalyst OS ソフトウェアを実行している Catalyst 6500/7600 デバイス。

ヒント　Catalyst 6500/7600 が Cisco IOS ソフトウェアを実行している場合は、[Router] タブでデバイスをルータとして追加します。[Cat6K] タブにデバイスを追加しないでください。

ナビゲーション パス

[IPSブロッキング（IPS Blocking）] ポリシーで、[ルータ（Router）]、[ファイアウォール（Firewall）]、または [Catalyst 6K] タブを選択し、[行の追加（Add Row）] ボタンをクリックするか、既存の行を選択して [行の編集（Edit Row）] ボタンをクリックします。ブロッキングポリシーを開く方法については、[Blocking] ページ （11 ページ）を参照してください。

フィールド リファレンス

表 5 : [Add Router Device]/[Modify Router Device]、[Add Firewall Device]/[Modify Firewall Device]、[Add Cat6K Device]/[Modify Cat6K Device] ダイアログボックス

要素	説明
IPアドレス	デバイスの IP アドレス。単一のホストアドレスが含まれたネットワーク/ホストポリシーオブジェクトのIPアドレスまたは名前を入力するか、[選択（Select）]をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成します。

要素	説明
Communication Type	ブロッキング デバイスへのログインに使用する通信メカニズム（[SSH 3DES]、[SSH DES]、[Telnet]）。デフォルトは [SSH 3DES] です。 [SSH 3DES] または [SSH DES] を選択した場合は、既知のホスト リストにデバイスを追加する必要があります。既知のホストリストにデバイスを追加する最も簡単な方法は、IPS Device Manager（IDM）を使用してセンサーにログインし、[設定（Configuration）]>[センサー管理（Sensor Management）] > [SSH] > [既知のホストキー（Known Host Keys）] > [既知のホストキーの追加（Add Known Host Key）] を選択して、デバイス アドレスを追加することです。または、センサーCLIにログインし、コンフィギュレーション モードを開始して、**ssh host-key** コマンドを使用することもできます。
NAT アドレス（NAT Address）	センサーとブロッキング デバイス間で NAT アドレスが使用されている場合、センサーのNATアドレス。単一のホストアドレスが含まれたネットワーク/ホストポリシーオブジェクトの NAT アドレスまたは名前を入力します。または、[選択（Select）]をクリックしてリストからオブジェクトを選択するか新しいオブジェクトを作成します。NAT が使用されない場合はデフォルトの 0.0.0.0 のままにします。
プロファイル名（Profile Name）	ブロッキングデバイスへのログインに使用するログインプロファイル。ブロッキング ポリシーの [User Profiles] タブでこのプロファイルを作成する必要があります。そうしないと、IPS はこのブロッキング デバイスを正常に使用できません。
Interfaces and directions where blocks will be applied（表） （ルータ専用）	ブロッキングまたはレート制限に使用する必要のあるデバイス上のインターフェイス。この表には、インターフェイス名、方向、およびIPS デバイスがブロッキング ACL に組み込む必要のある既存の ACL の名前が表示されます。 インターフェイスに、指定された方向の ACL がすでに設定されている場合は、ACL 名を pre-ACL または post-ACL として指定する必要があります。そうしないと、IPS によって ACL が削除されます。これらの ACL はブロッキングにだけ使用され、レート制限には使用されません。 • インターフェイスを追加するには、[行の追加（Add Row）] ボタンをクリックし、[ルータブロックインターフェイスの追加（Add Router Block Interface）] ダイアログボックスに入力します（[Add Router Block Interface]/[Modify Router Block Interface] ダイアログボックス（21 ページ）を参照）。 • インターフェイスを編集するには、インターフェイスを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • インターフェイスを削除するには、インターフェイスを選択し、[行を削除（Delete Row）] ボタンをクリックします。

要素	説明
Response Capabilities （ルータ専用）	このルータが実装できるアクション。複数のアクションを選択するには Ctrl を押しながらクリックします（強調表示されたアクションが選択されています）。次のオプションがあります。 • [ブロック（Block）]：ルータは、Request Block Connection アクションおよび Request Block Host アクションに対してブロックを実装できます。 • [レート制限（Rate Limit）]：ルータは、Request Rate Limit アクションに対してレート制限を実装できます。
VLANs where blocks will be applied（表） （Catalyst オペレーティング システムを実行している Catalyst 6500/7600 デバイスのみ）	ブロッキングに使用する必要のあるデバイス上の VLAN。この表には、VLAN 名と、IPS デバイスがブロッキング VACL に組み込む必要のある既存の VLAN ACL（VACL）の名前が表示されます。 VLAN に VACL がすでに設定されている場合は、VACL 名を pre-VACL または post-VACL として指定する必要があります。そうしないと、IPS によって VACL が削除されます。 • VLAN を追加するには、[行の追加（Add Row] ボタンをクリックし、[Cat6KブロックVLANの追加（Add Cat6K Block VLAN）] ダイアログボックスに入力します（[Add Cat6k Block VLAN]/[Modify Cat6k Block VLAN] ダイアログボックス （22 ページ）を参照）。 • VLAN を編集するには、その VLAN を選択して [行の編集（Edit Row）] ボタンをクリックします。 • VLAN を削除するには、その VLAN を選択して [行の削除（Delete Row）] ボタンをクリックします。

[Add Router Block Interface]/[Modify Router Block Interface] ダイアログボックス

[Add Router Block Interface]/[Modify Router Block Interface] ダイアログボックスを使用して、ルータ、または IPS ブロッキング デバイスとして設定されている IOS ソフトウェア Catalyst 6500/7600 デバイスに、ブロッキング インターフェイスを設定します。IPS センサーでは、ブロッキング アクションにインターフェイスが使用されます。

ナビゲーション パス

[ルータデバイスの追加（Add Router Device）]/[ルータデバイスの変更（Modify Router Device）] ダイアログボックスで、インターフェイス表の下の [行の追加（Add Row）] ボタンをクリックするか、表の行を選択して [行の編集（Edit Row）] ボタンをクリックします。[Add Router Device]/[Modify Router Device] ダイアログボックスを開く方法については、[Add Router Device]/[Modify Router Device]、[Add Firewall Device]/[Modify Firewall Device]、[Add Cat6K Device]/[Modify Cat6K Device] ダイアログボックス （19 ページ）を参照してください。

フィールド リファレンス

表 6 : [Add Router Block Interface]/[Modify Router Block Interface] ダイアログボックス

要素	説明
Interface Name	IPS がブロッキングに使用する必要のあるルータ上のインターフェイスの名前。ルータに設定されているとおり、名前を正確に入力します（たとえば、GigabitEthernet0/1 など）。
方向	ブロッキング ACL を適用する方向（[In] または [Out]）。

Pre ACL Name
Post ACL Name
	IPS がブロッキング アクションを実装するために作成するブロッキング エントリに結合する ACL。Pre ACL はブロッキング ACL の前に追加され、Post ACL はブロッキング ACL のあとに追加されます。詳細については、ルータおよびスイッチ ブロッキング デバイスについて （5 ページ）を参照してください。
	ヒント 指定した方向でインターフェイスに ACL を設定した場合は、[Pre ACL Name]/[Post ACL Name] フィールドに ACL の名前を指定する必要があります。そうしないと、ACL がインターフェイスから削除されます。インターフェイスと方向をブロッキングインターフェイスとして識別した場合、IPS はそのインターフェイス/方向で ACL を制御します。
	ブロッキングデバイスを Security Manager で管理している場合は、ブロッキングデバイスを選択し、[ツール（Tools）]>[設定のプレビュー（Preview Config）] を選択することで ACL 名を識別できます。インターフェイス設定で **ip access-group** コマンドを検索し、方向を確認します。たとえば、次の行は、CSM_FW_ACL_GigabitEthernet0/1 という名前の ACL が、GigabitEthernet0/1 インターフェイスに接続された In 方向に存在することを示しています。
	`interface GigabitEthernet0/1`
	`  ip access-group CSM_FW_ACL_GigabitEthernet0/1 in`
	この例では、ブロッキング インターフェイスとして GigabitEthernet0/1 を In 方向に設定する場合、pre-ACL または post-ACL として、CSM_FW_ACL_GigabitEthernet0/1 を必ず指定してください。ほとんどの場合は、ACL を post-ACL として指定します。これにより、比較的短い IPS ブロッキング ACL によって望ましくないトラフィックが最初に除外され、その後、ブロッキング デバイスによって他のアクセス ルールが実行されます。

[Add Cat6k Block VLAN]/[Modify Cat6k Block VLAN] ダイアログボックス

[Add Cat6k Block VLAN]/[Modify Cat6k Block VLAN] ダイアログボックスを使用して、Catalyst オペレーティング システムを実行し、IPS ブロッキング デバイスとして設定されている Catalyst 6500/7600 デバイスに、ブロッキング VLAN を設定します。IPS センサーでは、ブロッキング アクションに VLAN が使用されます。

ヒント　Catalyst 6500/7600 が Cisco IOS ソフトウェアを実行している場合は、デバイスを Cat6K ではなくルータとして追加します。

ナビゲーション パス

[Cat6Kデバイスの追加（Add Cat6K Device）]/[Cat6Kデバイスの変更（Modify Cat6K Device）] ダイアログボックスで、VLAN テーブルの下の [行の追加（Add Row）] ボタンをクリックするか、テーブルの行を選択して [行の編集（Edit Row）] ボタンをクリックします。[Add Cat6K Device]/[Modify Cat6K Device] ダイアログボックスを開く方法については、[Add Router Device]/[Modify Router Device]、[Add Firewall Device]/[Modify Firewall Device]、[Add Cat6K Device]/[Modify Cat6K Device] ダイアログボックス （19 ページ）を参照してください。

フィールド リファレンス

表 7 : [Add Cat6k Block VLAN]/[Modify Cat6k Block VLAN] ダイアログボックス

要素	説明
VLAN	IPS がブロッキングに使用する必要のある Catalyst 6500/7600 デバイス上の VLAN の数。数値は 1 ～ 4094 で指定でき、デバイスに定義されている必要があります。
Pre VACL Name Post VACL Name	IPS がブロッキング アクションを実装するために作成するブロッキング エントリに結合する VLAN ACL。Pre VACL はブロッキング VACL の前に追加され、Post VACL はブロッキング VACL のあとに追加されます。詳細については、ルータおよびスイッチ ブロッキング デバイスについて （5 ページ）を参照してください。 ヒント　VLAN に VACL を設定した場合は、[Pre VACL Name]/[Post VACL Name] フィールドに VACL の名前を指定する必要があります。そうしないと、VACL が VLAN から削除されます。VLAN をブロッキングインターフェイスとして指定した場合は、IPS によってその VLAN 上の VACL が制御されます。通常は、VACL 名を post-VACL として指定します。

[Add Never Block Host]/[Modify Never Block Host] または [Add Never Block Network]/[Modify Never Block Network] ダイアログボックス

[Add Never Block Host]/[Modify Never Block Host] または [Add Never Block Network]/[Modify Never Block Network] ダイアログボックスを使用して、ブロッキングの対象にしないホストまたはネットワークを指定します。ダイアログボックスの名前は、ホスト アドレスとネットワーク アドレスのどちらを追加するかを示します。

アドレスを指定するネットワーク/ホストポリシーオブジェクトのIPアドレスまたは名前を入力します。[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成することもできます。オブジェクトを選択した場合、オブジェクトには適切なタイプのエントリを 1 つ含めることができます。ホスト アドレスにはサブネット マスクがありませんが（たとえば10.100.10.1）、ネットワーク アドレスにはマスクがあります（たとえば 10.100.10.0/24）。

ナビゲーション パス

[IPSブロッキング（IPS Blocking）] ポリシーで、[ブロックしないホスト（Never Block Hosts）] タブまたは [ブロックしないネットワーク（Never Block Networks）] タブを選択し、[行の追加（Add Row）] ボタンをクリックするか、既存の行を選択して [行の編集（Edit Row）] ボタンをクリックします。ホストとネットワークは別々の表にリストされるため、目的の表に関連付けられているボタンをクリックしてください。ブロッキングポリシーを開く方法については、[Blocking] ページ （11 ページ）を参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。