インテリジェント アプリケーション バイパス

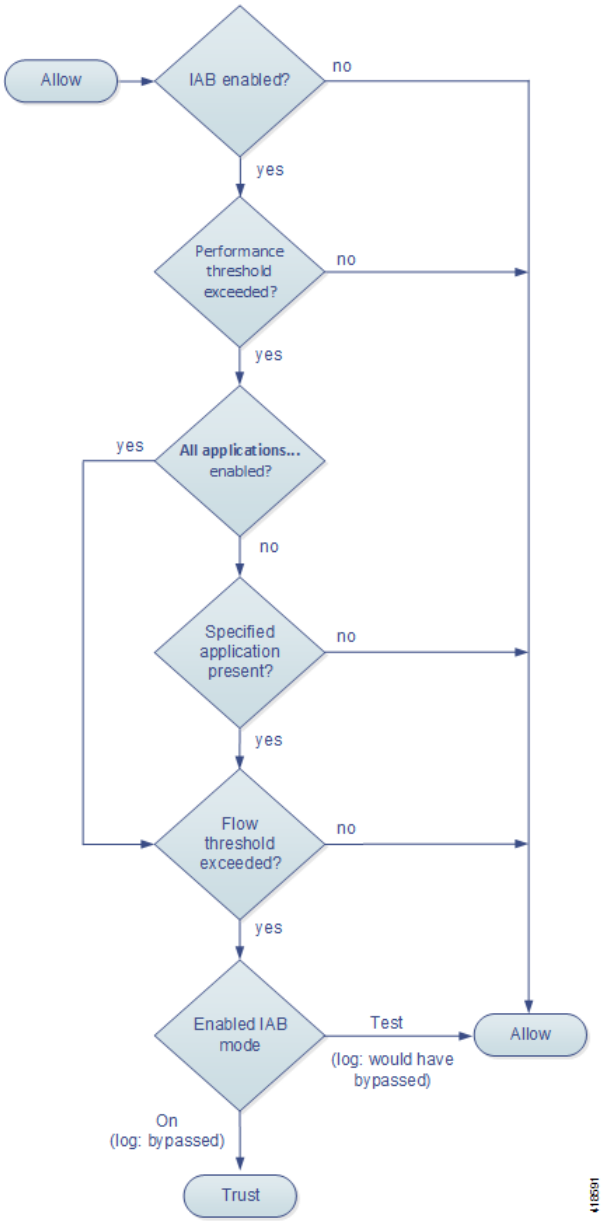
次の各トピックでは、インテリジェント アプリケーション バイパス の使用に向けてアクセス コントロール ポリシーを設定する方法を説明します。

IAB の概要

インテリジェント アプリケーション バイパス（IAB）では、パフォーマンスおよびフローのしきい値を超過した場合に、信頼できるものとしてさらなるインスペクションなしでネットワークを通過させるアプリケーションを指定します。たとえば、夜間バックアップがシステム パフォーマンスに著しい影響を及ぼす場合、しきい値を設定し、その値を超えたらバックアップ アプリケーションによって生成されるトラフィックを信頼するようにすることができます。オプションでは、インスペクション パフォーマンスしきい値を超過したときは、いずれかのフロー バイパスしきい値を超えるすべてのトラフィックを、アプリケーションのタイプに関係なく信頼するよう IAB を設定することができます。このオプションには、バージョン 6.1.0.3 または後続の 6.1.0.x パッチが必要です。

IAB は、アクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションによって許可されるトラフィックに対し、トラフィックが詳細なインスペクションの対象となる前に実行されます。テスト モードでは、しきい値を超過しているかどうか判断することと、しきい値を超過している場合、IAB を実際に有効化している状態（*バイパス モード*といいます）であればバイパスされたであろうアプリケーション フローを特定することが可能です。

次の図は、IAB の決定プロセスを示します。



IAB オプション

状態（State）

IAB を有効または無効にします。

パフォーマンス サンプル インターバル（Performance Sample Interval）

IAB パフォーマンス サンプリング スキャンの間隔を秒で指定します。この間隔で、システムは、IAB パフォーマンスしきい値と比較するためのシステム パフォーマンス測定値を収集します。値を 0 にすると、IAB は無効になります。

バイパス可能なアプリケーションとフィルタ（Bypassable Applications and Filters）

この機能には、相互に排他的な、次の 2 つのオプションがあります。

アプリケーション/フィルタ（Applications/Filters）

バイパス可能なアプリケーションおよびアプリケーションのセット（フィルタ）を指定できるエディタを提供します。指定の方法は、アクセス コントロール ルールでアプリケーション条件を指定するときとほぼ同じです。詳細については、アプリケーション トラフィックの制御（8-2 ページ）を参照してください。

未確認アプリケーションを含むすべてのアプリケーション（All applications including unidentified application）

インスペクション パフォーマンスしきい値を超過すると、アプリケーションのタイプに関係なく、いずれかのフロー バイパスしきい値を超過するすべてのトラフィックを信頼します。このオプションには、バージョン 6.1.0.3 か、後続の 6.1.0.x パッチが必要です。

インスペクション パフォーマンスしきい値（Inspection Performance Thresholds）

インスペクション パフォーマンスしきい値は、侵入インスペクションのパフォーマンスの限界を定めるもので、この限界を超えると、フローしきい値のインスペクションがトリガーされます。IAB では、0 に設定された インスペクション パフォーマンスしきい値は使用しません。

（注）　インスペクション パフォーマンスしきい値とフロー バイパスしきい値は、デフォルトでは無効化されています。IAB がトラフィックを信頼するには、少なくともいずれか 1 つを有効化し、いずれか 1 つを超過している必要があります。インスペクション パフォーマンスしきい値またはフロー バイパスしきい値を複数有効にした場合、IAB がトラフィックを信頼するには、いずれか 1 つのみを超過する必要があります。

ドロップ率（Drop Percentage）

消費が激しい侵入ルール、ファイル ポリシー、圧縮解除などによってパフォーマンス過負荷となったためにパケットがドロップされた場合にドロップされたパケットが、パケット全体に占める割合の平均。侵入ルールのような通常の設定によってドロップされるパケットは含まれません。1 より大きい整数を指定すると、指定されたパーセンテージのパケットがドロップされたときに IAB がアクティブ化することに注意が必要です。1 を指定すると、0 ～ 1 までのパーセンテージによって IAB がアクティブ化します。これにより、少ないパケット数で IAB がアクティブ化します。

プロセッサ使用率（Processor Utilization Percentage）

プロセッサ リソースの平均使用率。

パケット遅延（Package Latency）

マイクロ秒単位の平均パケット遅延。

フロー レート（Flow Rate）

1 秒あたりのフロー数で測定される、システムによるフロー処理率。このオプションでは、IAB は、フローを*件数*ではなく*レート*で測定するように設定されることに注意が必要です。

フロー バイパスしきい値（Flow Bypass Thresholds）

フロー バイパスしきい値はフローの限界を定めるもので、この限界を超えると、IAB は、バイパス モードではバイパス可能なアプリケーションを信頼し、テスト モードでは、アプリケーション トラフィックを許可してさらなるインスペクションの対象にします。IAB では、0 に設定された フロー バイパスしきい値は使用しません。

（注）　インスペクション パフォーマンスしきい値とフロー バイパスしきい値は、デフォルトでは無効化されています。IAB がトラフィックを信頼するには、少なくともいずれか 1 つを有効化し、いずれか 1 つを超過している必要があります。インスペクション パフォーマンスしきい値またはフロー バイパスしきい値を複数有効にした場合、IAB がトラフィックを信頼するには、いずれか 1 つのみを超過する必要があります。

フローあたりのバイト数

フローに含めることができる最大サイズ（KB）。

フローあたりのパケット数

フローに含めることができるパケットの最大個数。

フロー継続時間

フローをオープンのままにできる最長時間（秒）。

フロー速度

最大転送速度（KB/秒）。

IAB の設定

注意　IAB はすべての導入に必要なわけではなく、必要である場合も、限定的に使用されることがあります。ネットワーク トラフィック（特にアプリケーション トラフィック）とシステム パフォーマンス（予測可能なパフォーマンスの問題を含む）の専門知識がある場合を除き、IAB を有効化しないでください。IAB をバイパス モードで実行する場合は、指定したトラフィックを信頼することでリスクが生じないことを事前に確認してください。

しきい値を超過する場合に、信頼できるものとしてネットワークを通過させるアプリケーションを指定する方法:

手順 1　アクセス コントロール ポリシー エディタで [詳細設定（Advanced）] タブをクリックし、次に、[インテリジェント アプリケーション バイパス設定（Intelligent Application Bypass Settings）] の隣にある編集アイコン（  ）をクリックします。

代わりにビュー アイコン（  ）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する（Inherit from base policy）] をオフにして、編集を有効にします。

手順 2　IAB の各オプションを設定します。

- 状態（State）：IAB を [Off] または [On] にするか、IAB を [テスト（Test）] モードで有効にします。
- パフォーマンス サンプル間隔（Performance Sample Interval）：IAB のパフォーマンス サンプリング スキャンの間隔を秒単位で入力します。IAB を有効にする場合は、テスト モードであっても、0 以外の値を入力します。0 を入力すると、IAB が無効化されます。
- バイパス可能なアプリケーションとフィルタ（Bypassable Applications and Filters）：次のいずれかを実行します。
  - バイパスするアプリケーションとフィルタの数をクリックし、トラフィックをバイパスするアプリケーションを指定します。これは、アクセス コントロール ルールでアプリケーション条件を指定するときとほぼ同じ方法です。詳細については、アプリケーション トラフィックの制御（8-2 ページ）を参照してください。
  - [未確認アプリケーションを含むすべてのアプリケーション（All applications including unidentified applications）] をクリックし、インスペクション パフォーマンスしきい値を超過したときに、IAB が、いずれかのフロー バイパスしきい値を超えるすべてのトラフィックをアプリケーションのタイプに関係なく信頼するように設定します。このオプションには、バージョン 6.1.0.3 か、後続の 6.1.0.x パッチが必要です。
- インスペクション パフォーマンスしきい値（Inspection Performance Thresholds）：[設定（Configure）] をクリックし、しきい値を少なくとも 1 つ入力します。
- フロー バイパスしきい値（Flow Bypass Thresholds）：[設定（Configure）] をクリックし、しきい値を少なくとも 1 つ入力します。

少なくとも 1 つのインスペクション パフォーマンスしきい値と 1 つのフロー バイパスしきい値を指定する必要があります。IAB がトラフィックを信頼するには、両方を超過している必要があります。各タイプに複数のしきい値を入力した場合、いずれか 1 つのタイプのみを超過する必要があります。詳細については、IAB オプション（12-3 ページ）を参照してください。

手順 3　[OK] をクリックして、IAB 設定を保存します。

手順 4　[保存（Save）] をクリックして、ポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の展開（4-15 ページ）を参照してください。

IAB のロギングと分析

IAB は、接続終了イベントを強制的に生成します。それにより、接続のロギングを有効化しているかどうかに関係なく、バイパスされたフローおよびバイパスされたであろうフローがログに記録されます。接続イベントは、バイパス モードの場合はバイパスされたフロー、テスト モードの場合はバイパスされたであろうフローを示します。接続イベントに基づくカスタムのダッシュボード ウィジェットおよびレポートでは、バイパスされた、またはバイパスされたであろうフローの長期的な統計情報を表示できます。

IAB 接続イベント

アクション（Action）

[理由（Reason）] に「`Intelligent App Bypass`」が含まれる場合、次のいずれかです。

Allow：適用されている IAB 設定がテスト モードであり、[アプリケーション プロトコル（Application Protocol）] によって指定されたアプリケーションのトラフィックはインスペクション可能な状態のままであることを示します。

Trust：適用されている IAB 設定がバイパス モードであり、[アプリケーション プロトコル（Application Protocol）] によって指定されたアプリケーションのトラフィックが信頼され、さらなるインスペクションなしでネットワークを通過したことを示します。

理由（Reason）

「`Intelligent App Bypass`」は、バイパス モードまたはテスト モードの IAB によってイベントがトリガーされたことを示します。

アプリケーション プロトコル（Application Protocol）

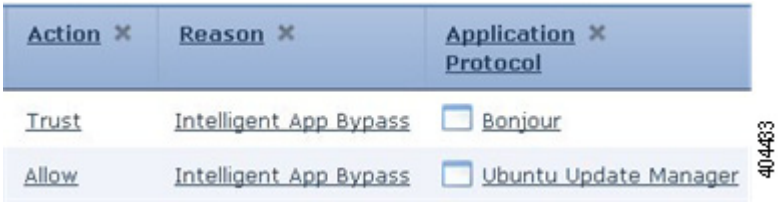
このフィールドには、イベントをトリガーしたアプリケーション プロトコルが表示されます。

例

次の図は切り取ったもので、一部のフィールドは省略されています。図には、2 つの別のアクセス コントロール ポリシーでの異なる IAB 設定から生じた 2 つの接続イベントの [アクション（Action）] フィールド、[理由（Reason）] フィールド、および [アプロケーション プロトコル（Application Protocol）] フィールドが示されています。

1 つ目のイベントでは、`Trust` アクションから、IAB がバイパス モードで有効化されており、Bonjour プロトコルのトラフィックが信頼され、さらなるインスペクションなしで通過したことが分かります。

2 つ目のイベントでは、`Allow` アクションから、IAB がテスト モードで有効化されているため、Ubuntu Update Manager のトラフィックはさらなるインスペクションの対象になったものの、IAB がバイパス モードであればバイパスされたであろうことが分かります。



例

次の図は切り取ったもので、一部のフィールドは省略されています。2 つ目のイベントのフローは、バイパスされており、(**アクション(Action)**：`Trust`、**理由(Reason)**：`Intelligent App Bypass`)、それとともに、侵入ルールによってインスペクションされています(**理由(Reason)**：`Intrusion Monitor`)。「`Intrusion Monitor`」という理由は、[イベントを生成する(Generate Events)] に設定された侵入ルールが接続中にエクスプロイトを検出したものの、ブロックはしなかったことを示しています。例では、これは、アプリケーションが検出される前に発生しています。アプリケーションの検出後、IAB は、アプリケーションをバイパス可能とみなし、フローを信頼しています。

Last Packet	Action	Reason	Application Protocol
2015-06-12 10:53:09	Trust	Intelligent App Bypass	Skype Probe
2015-06-12 10:53:08	Trust	Intelligent App Bypass, Intrusion Monitor	HTTP

404541

IAB カスタム ダッシュボード ウィジェット

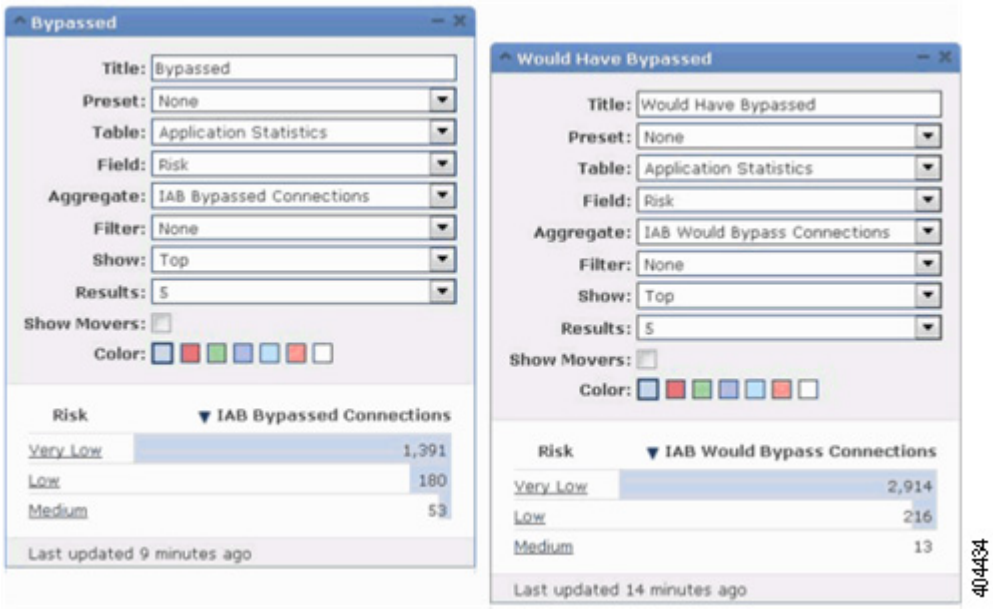
カスタムの分析ダッシュボード ウィジェットを作成し、接続イベントに基づく長期的な IAB 統計情報を表示することができます。このウィジェットを作成する際は、次の指定を行います。

- **プリセット(Preset)**：`None`
- **テーブル(Table)**：`Application Statistics`
- **フィールド(Field)**：`any`
- **集計(Aggregate)**：次のいずれか
  - `IAB Bypassed Connections`
  - `IAB Would Bypass Connections`
- フィルタ(Filter)：`any`

例

以下は、カスタム分析ダッシュボード ウィジェットの例です。

- *Bypassed* の例では、アプリケーションがバイパス可能と指定されており、展開されているアクセス コントロール ポリシーでは IAB がバイパス モードで有効にされているため、バイパスされたアプリケーション トラフィックの統計情報が表示されています。
- *Would Have Bypassed* の例では、アプリケーションがバイパス可能と指定されており、展開されているアクセス コントロール ポリシーでは IAB がテスト モードで有効にされているため、バイパスされたであろうアプリケーション トラフィックの統計情報が表示されています。



IAB カスタム レポート

カスタムのレポートを作成し、接続イベントに基づく長期的な IAB 統計情報を表示することができます。このレポートを作成する際は、次の指定を行います。

- テーブル（Table）：`Application Statistics`
- プリセット（Preset）：`None`
- フィルタ（Filter）：`any`
- X 軸（X-Axis）：`any`
- Y 軸（Y-Axis）：次のいずれか
  - `IAB Bypassed Connections`
  - `IAB Would Bypass Connections`

例

次の図は、2 つのレポートの例の抜粋を示します。

- *Bypassed* の例では、アプリケーションがバイパス可能と指定されており、展開されているアクセス コントロール ポリシーでは IAB がバイパス モードで有効にされているため、バイパスされたアプリケーション トラフィックの統計情報が表示されています。*Would Have Bypassed* の例では、アプリケーションがバイパス可能と指定されており、展開されているアクセス コントロール ポリシーでは IAB がテスト モードで有効にされているため、バイパスされたであろうアプリケーション トラフィックの統計情報が表示されています。