



インテリジェントアプリケーションバイパス

次のトピックでは、インテリジェントアプリケーションバイパス (IAB) を使用するようアクセスコントロールポリシーを設定する方法について説明します。

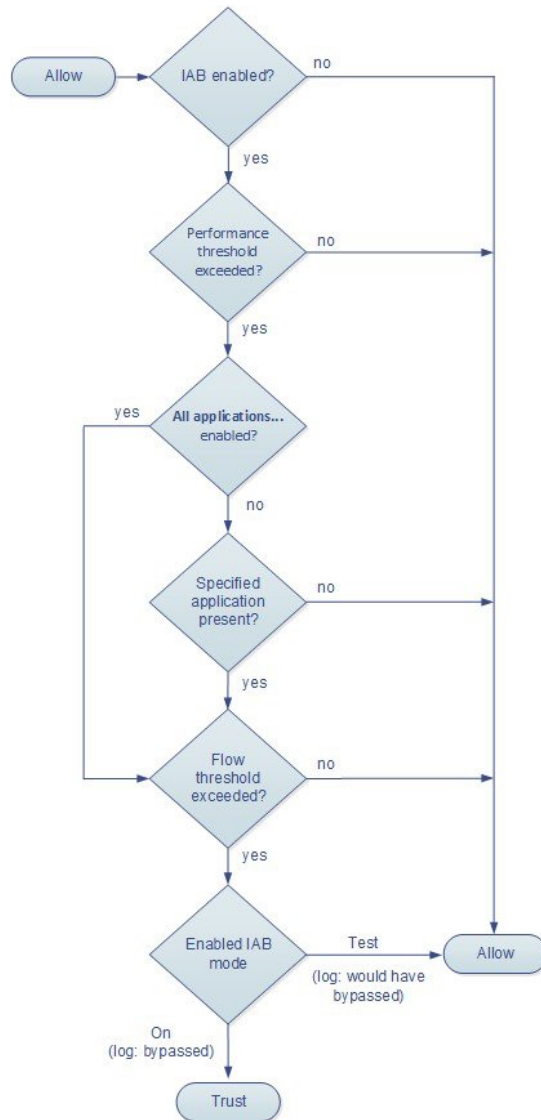
- [IAB の概要, 1 ページ](#)
- [IAB オプション, 2 ページ](#)
- [IAB の設定, 4 ページ](#)
- [IAB のロギングと分析, 6 ページ](#)

IAB の概要

IABは、パフォーマンスとフローのしきい値を超過した場合に追加のインスペクションなしでネットワークを通過する信頼されるアプリケーションを特定します。たとえば、毎晩のバックアップがシステムパフォーマンスに大きく影響する場合、しきい値を超えてもバックアップアプリケーションが生成したトラフィックを信頼するように設定できます。オプションで、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IABを設定できます。このオプションには、バージョン 6.0.1.4 か、後続の 6.0.1.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

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)

システムが IAB パフォーマンスしきい値との比較のためにシステム パフォーマンス メトリックを収集する IAB 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指定します。値を 0 にすると、IAB が無効になります。

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 (フィルタ) のセットを指定できるエディタが提供されます。 [アプリケーション条件 \(アプリケーション制御\)](#) 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

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。このオプションを使用するにはバージョン 6.0.1.4 またはそれ以降の 6.0.1.x パッチが必要です。

検査パフォーマンスしきい値 (Inspection Performance Thresholds)

検査パフォーマンスしきい値は、侵入検査パフォーマンスの限界を提供し、これを超えるとフローしきい値の検査が開始されます。IAB は、0 に設定されている検査パフォーマンスしきい値を使用しません。



(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、指定された割合のパケットがドロップされると IAB がアクティブになることに注意してください。1を指定すると、0～1の任意の割合によって IAB がアクティブになります。これにより、少数のパケットで IAB をアクティブにすることができます。

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ではフロー制限が提供され、これを超えると、IABがバイパスモードでバイパス可能なアプリケーショントラフィックを信頼するようにトリガーされるか、またはテストモードで追加の検査を受けるアプリケーショントラフィックが許可されます。IABは、0に設定されているフローバイパスしきい値を使用しません。



(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

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	任意 (Any)	任意 (Any)	Admin Access Admin Network Admin

**注意**

すべての展開に IAB が必要なわけではありません。IAB を使用する展開では、限定的な方法で IAB を使用場合があります。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。バイパス モードで IAB を実行する前に、指定したトラフィックを信頼してもリスクが発生しないことを確認します。

手順

- ステップ 1** アクセス コントロール ポリシー エディタで [詳細 (Advanced)] タブをクリックし、[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)] の横にある編集アイコン (✎) をクリックします。
- 代わりに表示アイコン (🔍) 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。
- ステップ 2** IAB のオプションを設定します。
- [状態 (State)] : IAB を [オフ (Off)] または [オン (On)]、あるいは [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 を有効にした場合は、テストモードであっても、ゼロ以外の値を入力します。0 を入力すると、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) : 次のいずれかを実行します。
 - バイパスされ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。[アプリケーション条件とフィルタの設定](#)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。このオプションを使用するにはバージョン 6.0.1.4 またはそれ以降の 6.0.1.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、1 つ以上のしきい値を入力します。
 - [フロー バイパスしきい値 (Flow Bypass Thresholds)] : [設定 (Configure)] をクリックし、1 つ以上のしきい値を入力します。

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。

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](#)、[\(2 ページ\)](#) を参照してください。

ステップ 3 [OK] をクリックして IAB 設定を保存します。

ステップ 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。[設定変更の導入](#)を参照してください。

IAB のロギングと分析

IAB は、接続ロギングを有効にしたかどうかを問わず、バイパスされたフローやバイパスされることが予想されるフローをロギングする接続終了イベントを強制します。接続イベントは、バイパスモードでバイパスされたフロー、またはテストモードでバイパスされることが予想されるフローを示します。接続イベントに基づいたカスタムのダッシュボードウィジェットやレポートでは、バイパスされたフローおよびバイパスされることが予想されるフローの長期的な統計情報を表示できます。

IAB の接続イベント

アクション (Action)

[理由 (Reason)] に [インテリジェントアプリケーションバイパス (Intelligent App Bypass)] が含まれる場合 :

許可 (Allow) :

適用された 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が、インスペクション用に使用可能のままであることを示します。

信頼する (Trust) :

適用された 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ているため、それ以上インスペクションが行われずにネットワークを通過することを示します。

理由 (Reason)

[インテリジェントアプリケーションバイパス (Intelligent App Bypass)] は、IAB がバイパスモードまたはテストモードでイベントをトリガーしたことを示します。

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

次の省略された図では、一部のフィールドが省かれています。図は、2つの別個のアクセス コ
ントロールポリシーの異なる IAB 設定から生成された2つの接続イベントの[アクション (Action)]、
[理由 (Reason)]、および[アプリケーションプロトコル (Application Protocol)]フィールドを示
しています。

最初のイベントの場合、[信頼する (Trust)]アクションは、IAB がバイパス モードで有効にされ
ており、Bonjour プロトコルトラフィックが信頼されているため、それ以上インスペクションが
行われずに受け渡されることを示します。

2番目のイベントの場合、[許可 (Allow)]アクションは、IAB がテストモードで有効にされてい
るため、Ubuntu Update Manager トラフィックはさらにインスペクションが行われる必要がありま
すが、IAB がバイパス モードであればバイパスされることが予想されることを示します。

Action ×	Reason ×	Application × Protocol
Trust	Intelligent App Bypass	<input type="checkbox"/> Bonjour
Allow	Intelligent App Bypass	<input type="checkbox"/> Ubuntu Update Manager

404483

例

次の省略された図では、一部のフィールドが省かれています。2番目のイベントのフローは両方
とも ([アクション (Action)]: [信頼する (Trust)]、[理由 (Reason)]: [インテリジェントア
プリケーションバイパス (Intelligent App Bypass)]) をバイパスし、侵入ルール ([理由 (Reason)]:
[侵入モニタ (Intrusion Monitor)]) によって検査されました。[侵入モニタ (Intrusion Monitor)]
の理由は、[イベントの生成 (Generate Events)]に設定された侵入ルールが検出されたが、接続時
にエクスプロイトをブロックしなかったことを示しています。この例では、これはアプリケーショ
ンが検出される前に発生しました。アプリケーションが検出された後、IAB は、アプリケーショ
ンがバイパス可能であると認識し、フローを信頼しました。

Last Packet ×	Action ×	Reason ×	Application × Protocol
2015-06-12 10:53:09	Trust	Intelligent App Bypass	<input type="checkbox"/> Skype Probe
2015-06-12 10:53:08	Trust	Intelligent App Bypass, Intrusion Monitor	<input type="checkbox"/> HTTP

404541

IAB のカスタム ダッシュボード ウィジェット

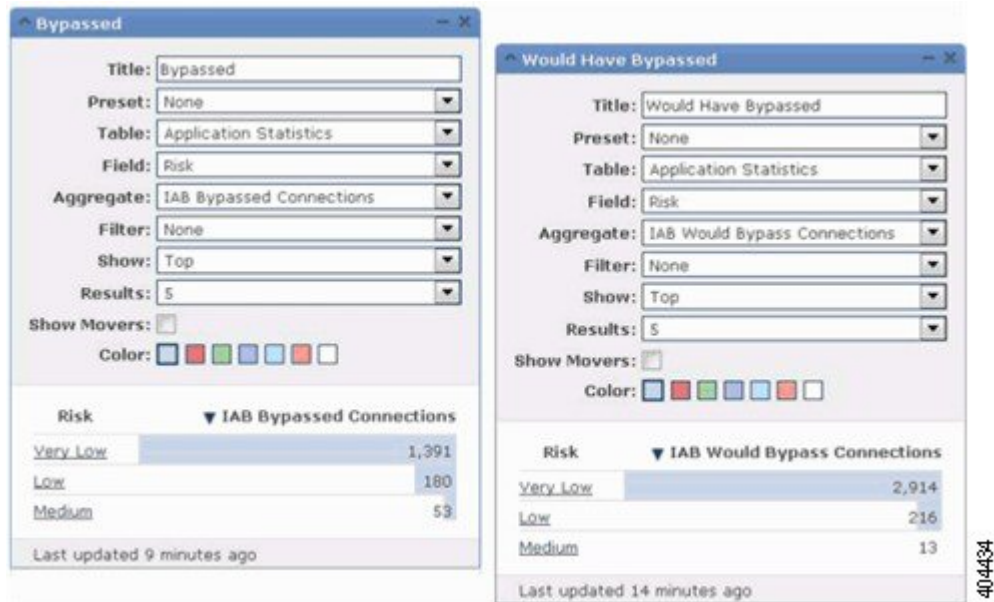
接続イベントに基づいて長期的な IAB の統計情報を表示するカスタム分析ダッシュボード ウィ
ジェットを作成できます。ウィジェットを作成するには、次の項目を指定します。

- プリセット (Preset) : なし (None)
- テーブル (Table) : アプリケーションの統計 (Application Statistics)
- フィールド (Field) : 任意 (any)
- 集約 (Aggregate) : 次のいずれか
 - IAB が接続をバイパスした (IAB Bypassed Connections)
 - IAB が接続をバイパスすることが予想された (IAB Would Bypass Connections)
- フィールド (Field) : 任意 (any)

例

次のカスタム分析ダッシュボードウィジェットの例では、次のようになっています。

- 「*Bypassed*」の例は、アプリケーションがバイパス可能として指定され、IAB が展開済みのアクセスコントロールポリシーにおいてバイパスモードで有効になっているためにバイパスされたアプリケーショントラフィックの統計を示しています。
- 「*Would Have Bypassed*」の例は、アプリケーションがバイパス可能として指定され、IAB が展開済みのアクセスコントロールポリシーにおいてテストモードで有効になっているためにバイパスされることが予想されたアプリケーショントラフィックの統計を示しています。



IAB のカスタム レポート

接続イベントに基づいて長期的な IAB の統計情報を表示するカスタムレポートを作成できます。レポートを作成する際には、次の項目を指定します。

- テーブル (Table) : アプリケーションの統計 (Application Statistics)
- プリセット (Preset) : なし (None)
- フィールド (Field) : 任意 (any)
- X 軸 (X-Axis) : 任意 (any)
- Y 軸 (Y-Axis) : 以下のいずれか
 - IAB が接続をバイパスした (IAB Bypassed Connections)
 - IAB が接続をバイパスすることが予想された (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*」の例は、アプリケーションがバイパス可能として指定され、IAB が展開済みのアクセスコントロールポリシーにおいてバイパスモードで有効になっているためにバイパスされたアプリケーショントラフィックの統計を示しています。
- 「*Would Have Bypassed*」の例は、アプリケーションがバイパス可能として指定され、IAB が展開済みのアクセスコントロールポリシーにおいてテストモードで有効になっているためにバイパスされることが予想されたアプリケーショントラフィックの統計を示しています。



