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。

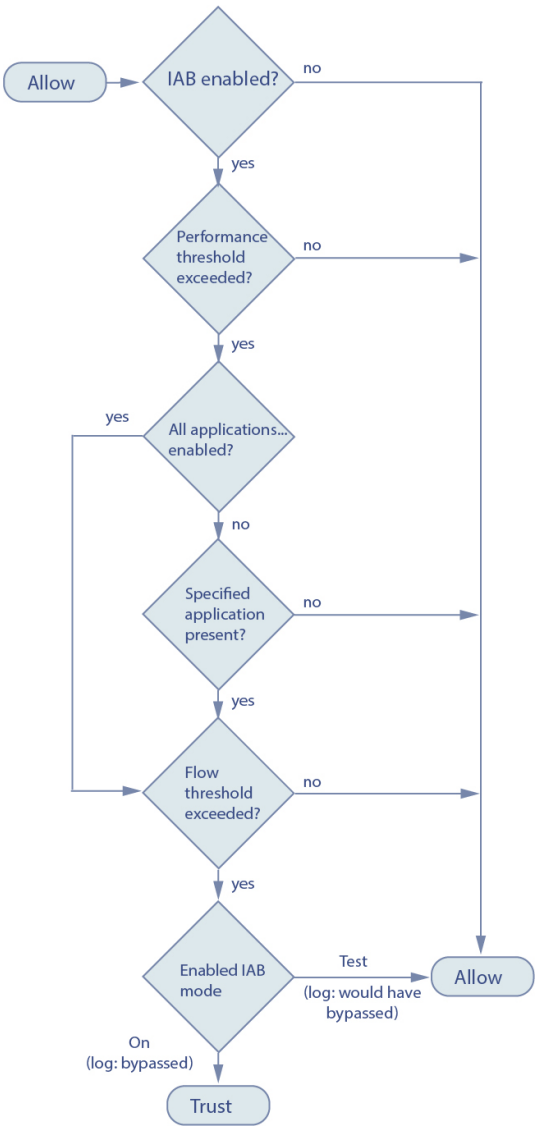
- IAB の概要 （1 ページ）
- IAB オプション （2 ページ）
- インテリジェント アプリケーション バイパスの要件と前提条件 （4 ページ）
- インテリジェント アプリケーション バイパスの設定 （4 ページ）
- IAB のロギングと分析 （6 ページ）

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。

システムはトラフィックがディープインスペクションの対象となる前に、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のアクションで許可されたトラフィック上で IAB を実行します。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。

次の図に、IAB の判断決定プロセスの説明を示します。



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。アプリケーションルール条件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。

パフォーマンスおよびフローのしきい値

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設定する必要があります。パフォーマンスしきい値を超えると、フローしきい値が検証され、1 つのしきい値を超えた場合には、指定されたトラフィックが信頼されます。複数を有効にする場合は、それぞれ 1 つだけを超過する必要があります。

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 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。次の 1 つまたは複数のインスペクション パフォーマンスしきい値を設定できます。

ドロップ率（Drop Percentage）

高価な侵入ルール、ファイル ポリシー、圧縮解除などによるパフォーマンスのオーバーロードのためにパケットがドロップされたときの、パケット全体に対する割合としてドロップされた平均パケット数。これは、侵入ルールなどの通常の設定によってドロップされたパケットを参照するものではありません。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）

使用されたプロセッサ リソースの平均比率。

パケット遅延

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 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。次の 1 つまたは複数のフロー バイパスしきい値を設定できます。

フローあたりのバイト数（Bytes per Flow）

フローに含めることができる最大キロバイト数。

フローあたりのパケット数（Packets per Flow）

フローに含めることができる最大パケット数。

フロー継続時間（Flow Duration）

フローを開いたままにできる最大秒数。

フロー速度（Flow Velocity）

最大転送速度（KB/秒）。

インテリジェントアプリケーションバイパスの要件と前提条件

モデルのサポート

任意（Any）

サポートされるドメイン

任意

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

インテリジェント アプリケーション バイパスの設定

⚠

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 を使用する場合があります。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、予測可能なパフォーマンスの問題の原因を含むシステム パフォーマンスの専門知識がない場合は、IAB を有効にしないでください。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。

始める前に

クラシックデバイスの場合は、制御ライセンスが必要です。

手順

ステップ 1 アクセス コントロール ポリシーのエディタで、パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [詳細設定（Advanced Settings）] をクリックします。次に、[インテリジェント アプリケーション バイパスの設定（Intelligent Application Bypass Settings）] の隣にある **[編集（Edit）]**（ ） をクリックします。

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）] に切り替えるか、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 スキャン間の時間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）]：次のいずれかを選択します。
  - 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。
- [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、両方を超過する必要があります。各タイプのしきい値を複数入力した場合は、各タイプの 1 つ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。

次のタスク

- アプリケーションが検出される前に一部のパケットの通過を許可する必要があるため、これらのパケットを検査するようにシステムを設定する必要があります。

  トラフィック識別の前に通過するパケットを処理するためのベストプラクティスおよびトラフィック識別の前に通過するパケットを処理するためのポリシーの指定を参照してください。

- 設定変更を展開します設定変更の展開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

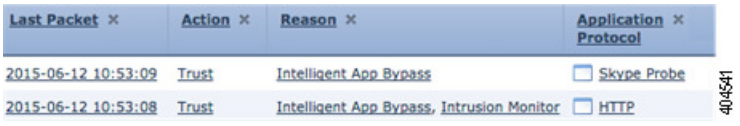
次の省略された図では、一部のフィールドが省かれています。図は、2 つの別個のアクセス コントロール ポリシーの異なる IAB 設定から生成された 2 つの接続イベントの [アクション（Action）]、[理由（Reason）]、および [アプリケーション プロトコル（Application Protocol）] フィールドを示しています。

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。

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。



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際には、次の項目を指定します。

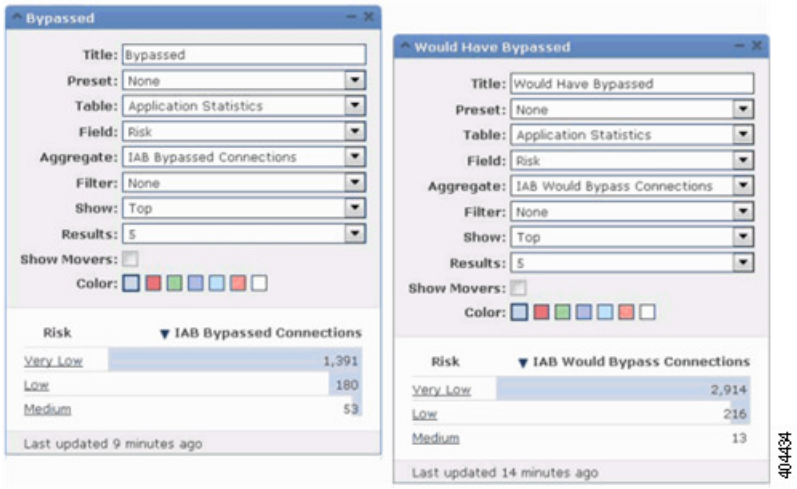
- プリセット（Preset）：なし（None）
- テーブル（Table）：**アプリケーションの統計（Application Statistics）**

- 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。

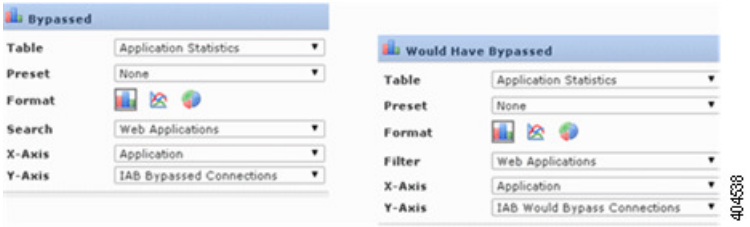
- テーブル（Table）：**アプリケーションの統計（Application Statistics）**
- プリセット（Preset）：なし（None）
- フィールド（Field）：任意（any）

- 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。



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。