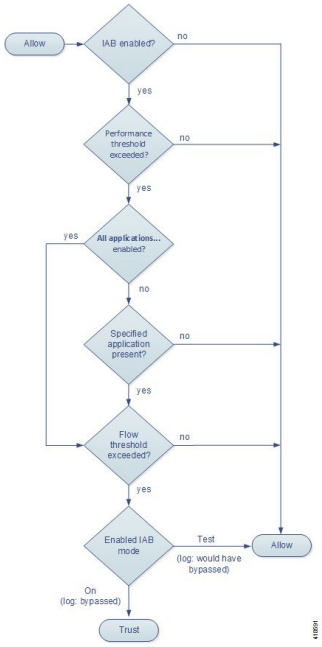
インテリジェント アプリケーション バイパス（IAB）

インテリジェントアプリケーションバイパス（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す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、しきい値を超えているかどうかを判断し、超えていた場合は、IABバイパスモードを有効にした場合にバイパスされたアプリケーションフローを特定できます。

次の図に、IAB意思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。

検査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）

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）

使用されたプロセッサ リソースの平均比率。

パッケージ遅延（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。このオプションを使用すると、フロー数ではなくフロー レートを測定するように IAB が設定されることに注意してください。.

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（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）。

IAB 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。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：

ステップ 1 アクセス コントロール ポリシー エディタで [Advanced] タブをクリックし、[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、設定の変更権限はありません。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 の各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 スキャン間の時間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）

[Reason] に [Intelligent App Bypass] が含まれる場合：

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）

[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、[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どちらもバイパス（[Action]：[Trust]、[Reason]：[Intelligent App Bypass]）されており、侵入ルール（[Reason]：[Intrusion Monitor]）によって検査されています。[Intrusion Monitor] の理由は、[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がブロックされ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

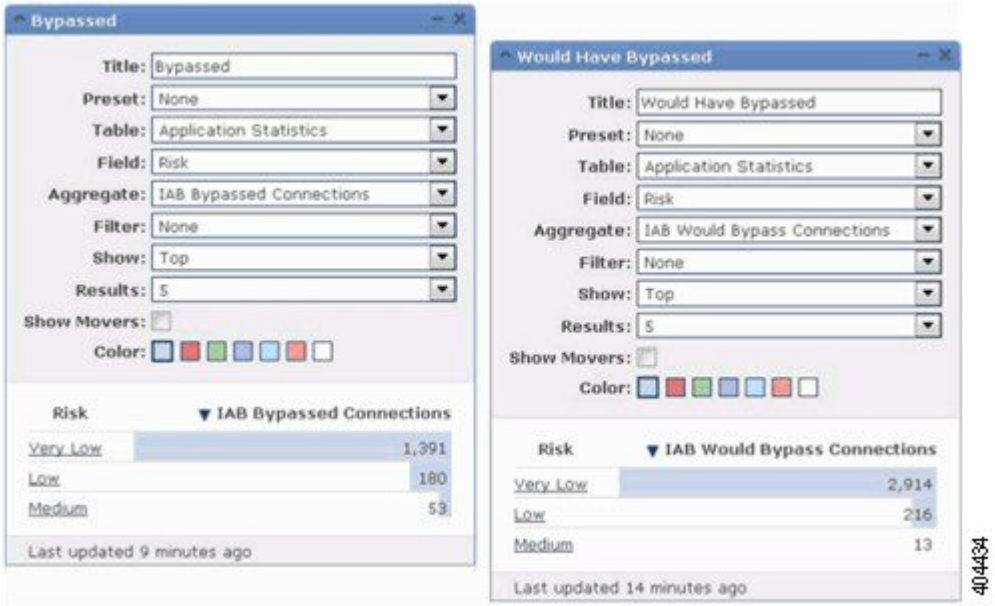
接続イベントに基づいて長期的なIABの統計情報を表示するカスタム分析ダッシュボード ウィジェットを作成できます。ウィジェットを作成する際には、次の項目を指定します。

- [Preset]：[None]
- [Table]：[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。

- [Table]：[Application Statistics]
- [Preset]：[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。


Bypassed
Table
Application Statistics
Preset
None
Format
Search
Web Applications
X-Axis
Application
Y-Axis
IAB Bypassed Connections
Would Have Bypassed
Table
Application Statistics
Preset
None
Format
Filter
Web Applications
X-Axis
Application
Y-Axis
IAB Would Bypass Connections
404538