デバイスのモニタリング

システムには、デバイスとデバイスを通過するトラフィックをモニタするために使用できるダッシュボードとイベント ビューアが含まれています。

トラフィック統計情を取得するためにロギングを有効にする

モニタリング ダッシュボードおよびイベント ビューアを使用して、幅広いトラフィック統計をモニタできます。ただし、どの統計情報を収集すべきかシステムに知らせるためにロギングを有効にする必要があります。

オプションの統計情報を収集し、イベントを生成するには、個別のアクセス ルール上で次のロギング タイプを有効にします。

- 接続ロギング：接続の最後でロギングを行うと、接続に関するほとんどの情報が提供されます。接続の開始も記録できますが、これらのイベントの情報は不完全です。接続ロギングはデフォルトで無効になっているため、追跡するトラフィックを対象とする各ルール（およびデフォルトのアクション）でこれを有効にする必要があります。
- ファイル ロギング：検出されたファイルに関する情報を収集するには、ファイル ロギングを有効にする必要があります。ファイル ロギングは、アクセス ルールでファイル ポリシーを選択すると自動的に有効になりますが、それを無効にすることもできます。

設定するロギングに加えて、禁止されたファイル、マルウェア、または侵入の試みをシステムが検出した場合には、ほとんどの接続（および接続の終了）を自動的にログに記録します。例外は、

デフォルト アクションによって処理される侵入イベントです。これらの侵入イベントを確認するには、デフォルト アクションで接続ロギングを有効にする必要があります。

ヒント

ロギング設定および関連する統計情報の評価を検討する際は、次のヒントに注目してください。

- アクセス コントロール ルールでトラフィックを許可すると、関連付けられた侵入ポリシーまたはファイル ポリシー（またはその両方）を使用して、さらにトラフィックをのインスペクションを実行し、トラフィックが最終宛先に到達する前に、侵入、禁止されたファイル、およびマルウェアをブロックすることができます。ただし、デフォルトでは、ファイルおよび侵入のインスペクションは暗号化されたペイロードでは無効になっていることに注意してください。侵入またはファイル ポリシーが接続をブロックする理由を発見した場合、接続ログ設定を問わず、システムは接続終了イベントをただちにログに記録します。ロギングが許可された接続は、ネットワーク内のトラフィックのほとんどの統計情報を提供します。
- 信頼されている接続は、信頼アクセス 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処理される接続です。ただし、信頼されている接続では、ディスカバリ データ、侵入、または禁止されたファイルやマルウェアがインスペクションされません。したがって、信頼されている接続の接続イベントには、限られた情報が含まれます。
- トラフィックをブロックするアクセス コントロール ルールおよびアクセス コントロール ポリシーのデフォルト アクションの場合は、システムは接続開始イベントをロギングします。一致するトラフィックは、追加のインスペクションなしで拒否されます。
- サービス妨害（DoS）攻撃の間にブロックされた TCP 接続をロギングすると、システム パフォーマンスに影響し、複数の同様のイベントによってデータベースが過負荷になる可能性があります。ブロック ルールにロギングを有効にする前に、そのルールがインターネット側のインターフェイスまたはDoS攻撃を受けやすい他のインターフェイス上のトラフィックをモニタするかどうかを検討します。

トラフィックのモニタリングおよびシステム ダッシュボード

システムには、デバイスを通過するトラフィックおよびセキュリティ ポリシーの結果を分析するために使用できる複数のダッシュボードがあります。ダッシュボード情報は、構成全体の有効性を評価し、ネットワークの問題を特定して解決するために使用します。

（注） トラフィック関連のダッシュボードに使用されるデータは、接続またはファイル ロギングを有効にするアクセス コントロール ルールから収集されます。ダッシュボードには、ロギングが有効になっていないルールと一致するトラフィックは反映されません。自分にとって重要な情報をログに記録するルールを設定してください。また、ユーザ情報はユーザ ID を収集するアイデンティティルールを設定している場合にのみ利用できます。さらに、侵入、ファイル、マルウェア、および Web カテゴリの情報は、それらの機能のライセンスがあり、機能を使用するルールを設定している場合のみ使用できます。

手順

ステップ 1 メイン メニューの [モニタリング（Monitoring）]をクリックして、[ダッシュボード（Dashboards）]ページを開きます。
ダッシュボードのグラフと表に表示されるデータを制御するために、定義済みの時間範囲（最後の時間や週など）を選択できます。また、特定の開始時刻と終了時刻を指定してカスタムの時間範囲を定義することもできます。

トラフィック関連のダッシュボードには、次のタイプの表示が含まれます。

- 上位 5 つの棒グラフ：これらのグラフは [ネットワークの概要（Network Overview）]ダッシュボードに表示されます。また、ダッシュボードテーブルで項目をクリックした場合、項目ごとのサマリのダッシュボードにも表示されます。[トランザクション（Transactions）]または [データの使用状況（Data Usage）]（送受信バイトの合計）のカウント間で情報を切り替えることができます。すべてのトランザクション、許可トランザクション、または拒否トランザクションを表示するために表示を切り替えることもできます。グラフと関連付けられている表を確認する場合は、[追加表示（View More）]をクリックします。
- 表：表には特定のタイプ（アプリケーションや Web カテゴリなど）の項目が、その項目の合計トランザクション、許可トランザクション、ブロックされたトランザクション、データの使用状況、送受信バイト数とともに表示されます。raw [値（Values）]と [パーセンテージ（Percentages）]間の数字は切り替えることができ、上位 10、100、または 1000 エントリが表示されます。項目がリンクの場合、そのリンクをクリックして、より詳細な情報が含まれているサマリ ダッシュボードを表示します。

ステップ 2 目次にある [ダッシュボード（Dashboard）]リンクをクリックして、次のデータのダッシュボードを表示します。

- [ネットワークの概要（Network Overview）]：ネットワークのトラフィックに関する概要情報が表示されます。情報には、一致したアクセスルール（ポリシー）、ユーザが送信側のトラフィック、接続で使用されているアプリケーション、一致した侵入シグネチャ、アクセスされた URL の Web カテゴリ、最も頻繁に接続されている宛先が含まれます。
- [ユーザ（Users）]：ネットワークの上位ユーザが表示されます。ユーザ情報を表示するには、アイデンティティ ポリシーを設定する必要があります。

- [アプリケーション（Applications）] : ネットワークで使用されている上位アプリケーション（Facebook など）が表示されます。この情報は、インスペクションを実行済みの接続にのみ提供されます。接続は、「許可」ルールと一致するか、またはゾーン、アドレス、およびポート以外の基準を使用するブロック ルールと一致するかどうかのインスペクションが実行されます。そのため、インスペクションが必要なルールにヒットする前に接続が信頼またはブロックされている場合、アプリケーション情報は使用できません。
- [Web カテゴリ（Web Categories）] : 訪問した Web サイトのカテゴリに基づいて、ネットワークで使用されている Web サイトの上位カテゴリ（ギャンブルや教育機関など）が表示されます。この情報を取得するためには、トラフィックの一致基準として Web カテゴリを使用するアクセス コントロール ルールが少なくとも 1 つ必要です。情報は、ルールに一致するトラフィック、またはルールに一致するかどうかを判断するためにインスペクションを実行する必要があるトラフィックに関してのみ提供されます。最初の Web カテゴリのアクセス コントロール ルールよりも前にあるルールと一致する接続に関するカテゴリ（またはレピュテーション）情報は表示されません。
- [ポリシー（Policies）] : 一致する上位のアクセス ルールがネットワーク トラフィック別に表示されます。
- [入力ゾーン（Ingress Zones）] : デバイスに入るトラフィックが通過する上位のセキュリティ ゾーンが表示されます。
- [出力ゾーン（Egress Zones）] : デバイスから出るトラフィックが通過する上位のセキュリティ ゾーンが表示されます。
- [宛先（Destinations）]ネットワーク トラフィックの上位の宛先が表示されます。
- [攻撃者（Attackers）] : 侵入イベントをトリガーする接続の送信元である上位の攻撃者が表示されます。この情報を表示するには、アクセス ルールに侵入ポリシーを設定する必要があります。
- [ターゲット（Targets）] : 攻撃の被害者である、侵入イベントの上位のターゲットが表示されます。この情報を表示するには、アクセス ルールに侵入ポリシーを設定する必要があります。
- [脅威（Threats）]トリガーされた上位の侵入ルールが表示されます。この情報を表示するには、アクセス ルールに侵入ポリシーを設定する必要があります。
- [ファイル ログ（File Logs）] : ネットワーク トラフィックで確認された上位のファイル タイプが表示されます。この情報を表示するには、アクセス ルールにファイル ポリシーを設定する必要があります。
- [システム（System）] : インターフェイスとインターフェイスのステータス（IP アドレスを確認するには、そのインターフェイスにマウスオーバーします）、システムの全体的なスループット、およびシステム イベント、CPU 使用率、メモリ使用率、ディスク使用率に関する概要情報など、システムの全体的情報が表示されます。すべてのインターフェイスではなく特定のインターフェイスを表示するように、スループット グラフを制限できます。

（注） [システム（System）] ダッシュボードに表示される情報は、全体的なシステム レベルの情報です。デバイスの CLI にログインすると、さまざまなコマンドを使用して詳細情報を確認できます。たとえば、**show cpu** および **show memory** コマンドにはその他の詳細を表示するためのパラメータがありますが、これらのダッシュボードには、**show cpu system** および **show memory system** コマンドからのデータが表示されます。

ステップ 3 目次でこれらのリンクをクリックすることもできます。

- [イベント（Events）] : イベント発生時にイベントが表示する場合に選択します。個々のアクセス ルールに関連する接続イベントを表示するには、それぞれのアクセス ルールで接続のロギングを有効にする必要があります。これらのイベントは、ユーザの接続の問題を解決するのに役立ちます。

コマンドラインを使用したその他の統計情報のモニタリング

Firepower Device Manager ダッシュボードには、デバイスを介して移動するトラフィックや一般的なシステム使用状況に関連するさまざまな統計情報が表示されます。ただし、デバイス CLI にログインすることによって、ダッシュボードには表示されていない領域のその他の情報を取得できます（CLI（コマンドライン インターフェイス）へのログインを参照）。

CLI には、これらの統計情報を表示するためのさまざまな **show** コマンドが含まれています。また、**ping** や **traceroute** などのコマンドを含め、一般的なトラブルシューティングに CLI を使用することもできます。ほとんどの **show** コマンドには、統計を 0 にリセットするための対になった **clear** コマンドがあります。

コマンドについては、『*Command Reference for Firepower Threat Defense*』（http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html）を参照してください。

たとえば、次のコマンドが役に立ちます。

- **show nat** は、NAT ルールのヒット数を表示します。
- **show xlate** は、アクティブな実際の NAT 変換を表示します。
- **show conn** は、デバイスを介して行われる現在の接続に関する情報を表示します。
- **show dhcpd** は、インターフェイスで設定した DHCP サーバに関する情報を表示します。
- **show interface** は、各インターフェイスの使用状況の統計を表示します。

イベントの表示

ロギングを有効にしたアクセス ルールから生成されたイベントを表示できます。イベントはまた、トリガーされた侵入ポリシーとファイル ポリシーについても生成されます。

イベント ビューアテーブルには、生成されたイベントがリアルタイムで表示されます。新しいイベントが生成されると、古いイベントはテーブルからロール アウトされます。

はじめる前に

特定のタイプのイベントが生成されるかどうかは、関連するポリシーに一致する接続に加え、次のことに依存します。

- 接続イベント：アクセス ルールは接続ロギングを有効にする必要があります。
- 侵入イベント：アクセス ルールは侵入ポリシーを適用する必要があります。
- ファイルおよびマルウェア イベント：アクセス ルールはファイル ポリシーを適用し、ファイル ロギングを有効にする必要があります。

手順

ステップ 1 メイン メニューの [監視（Monitoring）]をクリックします。

ステップ 2 目次から [イベント（Events）]を選択します。
イベント ビューアは、イベント タイプに基づいて、タブ上のイベントを整理します。詳細については、イベント タイプ，（7 ページ）を参照してください。

ステップ 3 表示するイベント タイプのタブをクリックします。
イベント リストでは、次の操作を実行できます。

- イベントをより簡単に検索、分析できるようにするために、新しいイベントの追加を停止するには、[一時停止（Pause）]をクリックします。新しいイベントが表示されるようにするには、[再開（Resume）]をクリックします。
- 新しいイベントの表示速度を制御するには、別のリフレッシュ レート（5、10、20、60 秒）を選択します。
- 必要なカラムを含むカスタム ビューを作成します。カスタム ビューを作成するには、タブバーの [+]ボタンをクリックするか、[カラムの追加/削除（Add/Remove Columns）] をクリックします。事前設定されたタブは変更できないため、カラムを追加または削除すると新しいビューが作成されます。詳細については、カスタム ビューの設定，（8 ページ）を参照してください。
- カラム幅を変更するには、カラム ヘッダーの境界をクリックし、目的の幅までドラッグします。

- イベントに関する詳細情報を表示するには、イベントの上にカーソルを置き、[詳細の表示（View Details）]をクリックします。イベントの各フィールドの説明については、イベントフィールドの説明，（10 ページ）を参照してください。

ステップ 4 必要に応じてテーブルにフィルタを適用すると、さまざまなイベント属性に基づき目的のイベントを見つけることができます。
新規フィルタを作成するには、ドロップダウンリストからアトミック要素を選択してフィルタを手動で入力し、フィルタの値を入力するか、フィルタリングの基準となる値を含むイベント テーブルのセルをクリックしてフィルタを作成します。同じカラムにある複数のセルをクリックして値の間に OR 条件を作成するか、異なるカラムにあるセルをクリックしてカラムの間に AND 条件を作成することができます。セルをクリックしてフィルタを作成した場合は、得られたフィルタを編集して、適切に調整することもできます。フィルタ ルールの作成の詳細については、イベントのフィルタリング，（9 ページ）を参照してください。

フィルタを作成したら、次のいずれかを実行します。

- フィルタを適用してテーブルを更新し、フィルタと一致するイベントのみが表示されるようにするには、[フィルタ（Filter）]ボタンをクリックします。
- 適用したフィルタをすべてクリアして、フィルタリングされていない状態のテーブルに戻るには、[フィルタ（Filter）]ボックスの [フィルタのリセット（Reset Filters）] をクリックします。
- フィルタのいずれかのアトミック要素をクリアするには、要素の上にカーソルを置き、要素の [X]をクリックします。さらに [フィルタ（Filter）]ボタンをクリックします。

イベント タイプ

システムは次の種類のイベントを生成できます。モニタリング ダッシュボードでこの情報に関連する統計情報を確認するには、次のイベントを生成する必要があります。

接続イベント

ユーザがシステムを通過するトラフィックを生成するときの接続イベントを生成できます。アクセス ルールで接続のロギングを有効化している場合のみ、接続イベントを確認できます。

接続イベントには、送信元および宛先 IP アドレスとポート、使用される URL およびアプリケーション、送信されるバイト数またはパケット数など、接続に関するさまざま情報が含まれています。この情報には、実行したアクション（たとえば接続の許可またはブロック）、接続に適用されるポリシーなども含まれます。

侵入イベント

システムは、ネットワークを通過するパケットのインスペクションを実行し、ホストとそのデータの可用性、整合性、および機密性に影響を与える可能性がある悪意のあるアクティビティについて調べます。システムは、侵入の可能性を特定すると侵入イベントを生成します。これは、エクスプロイトの日付、時刻、タイプ、および攻撃元とそのターゲットに関するコンテキスト情報の記録です。

ファイル イベント

ファイル イベントは、ファイル ポリシーに基づいてシステムがネットワーク トラフィック内で検出した（およびオプションでブロックした）ファイルを表します。これらのイベントを生成するには、ファイル ポリシーを適用するアクセス ルールでファイルのロギングを有効にする必要があります。

システムがファイル イベントを生成するときは、呼び出しを行うアクセス コントロール ルールのロギング設定に関係なく、関連する接続の終了も記録します。

マルウェア イベント

システムは、全体的なアクセス コントロール設定の一環として、ネットワーク トラフィックのマルウェアを検出できます。AMP for Firepower は、結果として生じたイベントの性質や、いつどこでどのようにしてマルウェアが検出されたかに関するコンテキスト データを含むマルウェア イベントを生成できます。これらのイベントを生成するには、ファイル ポリシーを適用するアクセス ルールでファイルのロギングを有効にする必要があります。

カスタム ビューの設定

独自のカスタム ビューを作成して、イベントの表示に必要なカラムが簡単に表示されるようにすることができます。また、事前定義ビューは編集または削除できませんが、カスタム ビューは編集または削除できます。

手順

ステップ 1 [モニタリング（Monitoring）] > [イベント（Events）] を選択します。

ステップ 2 次のいずれかを実行します。

- 既存のカスタム（または事前定義された）ビューに基づいて新規ビューを作成するには、そのビューのタブをクリックしてから、ビュータブの左側にある [+]ボタンをクリックします。
- 既存のカスタム ビューを編集するには、そのビューのタブをクリックします。

（注） カスタム ビューを削除するには、ビューのタブにある [X]ボタンをクリックします。削除すると、元に戻すことはできません。

ステップ 3 右側のイベント テーブルの上にある [追加/削除カラム（Add/Remove Columns）]アイコン ボタンをクリックし、選択したリストに、ビューに含めるカラムのみが含まれるようになるまで、カラムを選択または選択解除します。
使用可能な（ただし使用されていない）リストと選択されているリストの間で、カラムをクリックしてドラッグします。選択されているリスト内でカラムをクリックしてドラッグし、左から右に向かうテーブル内でのカラムの順番を変更することもできます。カラムについては、イベント フィールドの説明, （10 ページ）を参照してください。

完了したら [OK]をクリックして、カラムの変更を保存します。

（注） 事前定義されたビューを表示しながらカラムの選択を変更すると、新規ビューが作成されます。

ステップ 4 必要に応じてカラムのセパレータをクリックしてドラッグし、カラムの幅を変更します。

イベントのフィルタリング

複雑なフィルタを作成してイベント テーブルを制限し、現在関心のあるイベントのみが表示されるようにできます。次の手法を単独または組み合わせて使用して、フィルタを作成できます。

カラムのクリック

フィルタを作成する最も簡単な方法は、フィルタリングの基準となる値を含むイベント テーブルのセルをクリックすることです。セルをクリックすると、その値とフィールドの組み合わせに正しく定式化されているルールを使用して、[フィルタ（Filter）]フィールドが更新されます。ただし、この手法を使用するには、イベントの既存のリストに目的の値が含まれている必要があります。

すべてのカラムをフィルタリングすることはできません。セルのコンテンツをフィルタリングできる場合は、そのセルの上にカーソルを合わせたときに下線が表示されます。

アトミック要素の選択

[フィルタ（Filter）]フィールドをクリックして、ドロップダウンから目的のアトミック要素を選択した後、照合値を入力することでフィルタを作成することもできます。これらの要素には、イベント テーブルのカラムとして表示されないイベント フィールドが含まれます。また、表示するイベントと入力された値との関係を定義するオペレータが含まれます。カラムをクリックすると必ず、「equals (=)」フィルタが表示されますが、要素を選択すると、数値フィールドに「greater than (>)」または「less than (<)」も選択できるようになります。

[フィルタ（Filter）]フィールドに要素を追加する方法に関係なく、フィールドに入力してオペレータまたは値を調整できます。テーブルにフィルタを適用するには、[フィルタ（Filter）]をクリックします。

イベント フィルタの演算子

イベント フィルタには、次の演算子を使用できます。

=	等しい。イベントは指定した値と一致します。ワイルドカードを使用することはできません。
!=	等しくない。イベントは指定した値と一致しません。「等しくない」の式を作成するには、感嘆符（!）を入力する必要があります。
>	次の値より大きい。イベントに、指定した値よりも大きい値が含まれます。この演算子はポートや IP アドレスなど、数値のみに使用できます。
<	次の値より小さい。イベントに、指定した値よりも小さい値が含まれます。この演算子は、数値のみに使用できます。

複雑なイベント フィルタのルール

複数のアトミック要素を含む複雑なフィルタを作成する場合、次のルールに注意してください。

- 同じタイプの要素には、そのタイプのすべての値の間に OR 関係があります。たとえば、Initiator IP=10.100.10.10 と Initiator IP=10.100.10.11 を含めると、送信元としてこれらのいずれかのアドレスを持つイベントが照合されます。
- 異なるタイプの要素には、AND 関係があります。たとえば、Initiator IP=10.100.10.10 と Destination Port/ICMP Type=80 を含めると、この送信元アドレスと宛先ポートのみを持つイベントが照合されます。10.100.10.10 から異なる宛先ポートへのイベントは表示されません。
- IPv4 アドレスや IPv6 アドレスなどの数値要素は範囲を指定できます。たとえば、Destination Port=50-80 を指定して、この範囲内のポートのすべてのトラフィックを取得できます。ハイフンを使用して、開始と終了の数字を区切ります。すべての数値フィールドに対して、範囲を使用できるわけではありません。たとえば、[送信元（Source）] 要素に IP アドレスを範囲で指定することはできません。
- ワイルドカードまたは正規表現は使用できません。

イベント フィールドの説明

イベントには次の情報が含まれます。これらの情報は、イベントの詳細情報を表示すると確認できます。また、イベント ビューア表に列を追加すると、最も関心のある情報を表示することができます。

以下に、使用可能なフィールドの完全なリストを示します。すべてのフィールドがどのイベントタイプにも適用されるわけではありません。個別のイベントで利用可能な情報は、システムがいつ、なぜ、どのようにして接続を記録したかによって異なることに注意してください。

操作

接続イベントの場合、接続をロギングしたアクセス コントロール ルールまたはデフォルト アクションに関連付けられたアクション。

許可（Allow）

明示的に許可された接続。

信頼（Trust）

信頼できる接続。最初のパケットが信頼ルールによって検出されたTCP接続のみ、接続終了イベントを生成します。システムは、最後のセッション パケットの1時間後にイベントを生成します。

ブロック（Block）

ブロックされている接続。[ブロック（Block）]動作は、次の条件下で、アクセス許可ルールに関連付けることができます。

- 侵入ポリシーによってエクスプロイトが検出された接続。
- ファイルがファイル ポリシーによってブロックされている接続。

デフォルト アクション（Default Action）

接続はデフォルト アクションによって処理されました。

ファイル イベントまたはマルウェア イベントの場合、ファイルが一致したルールのルール アクションに関連付けられているファイル ルール アクションと、関連するファイル ルール アクションのオプション。

許可された接続（Allowed Connection）

システムがイベントのトラフィック フローを許可したかどうか。

アプリケーション（Application）

接続で検出されたアプリケーション。

アプリケーションのビジネスとの関連性（Application Business Relevance）

接続で検出されたアプリケーション トラフィックに関連するビジネス関連性：Very High、High、Medium、Low、または Very Low。接続で検出されたアプリケーションのタイプごとに、関連するビジネス関連性があります。このフィールドでは、それらのうち最も低いもの（関連が最も低い）が表示されます。

アプリケーション カテゴリ、アプリケーション タグ（Application Categories、Application Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

アプリケーションのリスク（Application Risk）

接続で検出されたアプリケーション トラフィックに関連するリスク：Very High、High、Medium、Low、または Very Low。接続で検出されたアプリケーションのタイプごとに、関連するリスクがあります。このフィールドでは、それらのうち最も高いものが表示されます。

ブロック タイプ（Block Type）

イベントのトラフィック フローと一致するアクセス コントロール ルールで指定されたブロックのタイプ。ブロックまたはインタラクティブ ブロック。

クライアント アプリケーション（Client Application）、クライアント バージョン（Client Version）

接続で検出されたクライアントのクライアント アプリケーションとバージョン。

クライアントのビジネスとの関連性（Client Business Relevance）

接続で検出されたクライアント トラフィックに関連するビジネス関連性：Very High、High、Medium、Low、または Very Low。接続で検出されたクライアントのタイプごとに、ビジネスとの関連性が関連付けられています。このフィールドは、最も低いもの（関連性が最も低い）を表示します。

クライアント カテゴリ、クライアント タグ（Client Category、Client Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

クライアント リスク（Client Risk）

接続で検出されたクライアント トラフィックに関連するリスク：Very High、High、Medium、Low、または Very Low。接続で検出されたクライアントのタイプごとに、リスクが関連付けられています。このフィールドは、最も高いものを表示します。

接続（Connection）

内部的に生成されたトラフィック フローの固有 ID。

接続ブロックタイプ インジケータ（Connection Blocktype Indicator）

イベントのトラフィック フローと一致するアクセス コントロール ルールで指定されたブロックのタイプ。ブロックまたはインタラクティブ ブロック。

接続バイト（Connection Bytes）

接続の合計バイト数。

接続時間（Connection Time）

接続の開始時刻。

接続タイムスタンプ（Connection Timestamp）

接続が検出された時刻。

拒否された接続（Denied Connection）

システムがイベントのトラフィック フローを拒否したかどうか。

宛先の国または大陸（Destination Country and Continent）

受信ホストの国および大陸。

宛先 IP（Destination IP）

受信ホストの IP アドレス。

宛先ポート/ICMP コード、宛先ポート、宛先 Icode（Destination Port/ICMP Code：Destination Port： Destination Icode）

セッション レスポンダが使用するポートまたは ICMP コード。

方向（Direction）

ファイルの送信方向。

傾向（Disposition）

ファイルの性質。

マルウェア（Malware）

AMP クラウドでそのファイルがマルウェアとして分類されていること、またはファイルの脅威スコアが、ファイル ポリシーで定義されたマルウェアしきい値を超えていることを示します。

正常（Clean）

AMP クラウドがファイルを正常に分類したことを示します。

不明（Unknown）

システムが AMP クラウドに問い合わせましたが、ファイルの性質が割り当てられていませんでした。言い換えると、AMP クラウドがファイルを正しく分類していませんでした。

応対不可（Unavailable）

システムがAMPクラウドに問い合わせできなかったことを示します。この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。

該当なし

[ファイル検出（Detect Files）] または [ファイル ブロック（Block Files）] ルールがファイルを処理し、システムが AMP クラウドに問い合わせなかったことを示します。

出力インターフェイス、出力セキュリティ ゾーン（Egress Interface、Egress Security Zone）

接続がデバイスを通り抜けたゾーンとインターフェイス。

イベント、イベント タイプ（Event、Event Type）

イベントのタイプ。

イベント秒、イベント マイクロ秒（Event Seconds、Event Microseconds）

イベントが検出された時刻（秒またはマイクロ秒単位）。

ファイル カテゴリ（File Category）

ファイル タイプの一般的なカテゴリ（Office ドキュメント、アーカイブ、マルチメディア、実行可能ファイル、PDF ファイル、エンコード ファイル、グラフィック、システム ファイルなど）。

ファイル イベント タイムスタンプ（File Event Timestamp）

ファイルまたはマルウェア ファイルが作成された日時。

ファイル名（File Name）

ファイルの名前です。

ファイル ルールのアクション（File Rule Action）

ファイルを検出したファイル ポリシー ルールに関連したアクション、および関連するファイル アクション オプション。

ファイル SHA256（File SHA256）

ファイルの SHA-256 ハッシュ値。

ファイル サイズ（File Size）（KB）

ファイルのサイズ（KB 単位）。システムがファイルを完全に受信する前にブロックした場合、ファイル サイズが空白になる場合があります。

ファイル タイプ（File Type）

ファイルのタイプ（HTML や MSEXE など）。

ファイル/マルウェア ポリシー（File/Malware Policy）

イベントの生成に関連付けられているファイル ポリシー。

ファイルログ ブロックタイプ インジケータ（Filelog Blocktype Indicator）

イベントのトラフィック フローと一致するファイル ルールで指定されたブロックのタイプ。ブロックまたはインタラクティブ ブロック。

ファイアウォール ポリシー ルール、ファイアウォール ルール（Firewall Policy Rule、Firewall Rule）

接続を処理したアクセス コントロール ルールまたはデフォルト アクション。

最初のパケット（First Packet）

セッションの最初のパケットが検出された日時。

HTTP リファラ（HTTP Referrer）

接続で検出された HTTP トラフィックの要求 URL のリファラを示す HTTP リファラ（他の URL へのリンクを提供した Web サイト、他の URL からリンクをインポートした Web サイトなど）。

HTTP レスポンス（HTTP Response）

クライアントからの接続経由の HTTP 要求に応じて送信される HTTP ステータス コード。

IDS の分類（IDS Classification）

イベントを生成したルールが属する分類。

入力インターフェイス、入力セキュリティ ゾーン（Ingress Interface、Ingress Security Zone）

接続がデバイスに入ったゾーンとインターフェイス。

イニシエータ バイト、イニシエータ パケット（Initiator Bytes、Initiator Packets）

セッション イニシエータが送信した合計バイト数またはパケット数。

イニシエータの国または大陸（Initiator Country and Continent）

セッションを開始したホストの所在地の国と地域の名前。イニシエータの IP アドレスがルーティング可能であるときにのみ使用できます。

イニシエータ IP（Initiator IP）

セッションを開始したホスト IP アドレス（および DNS 解決が有効化されている場合はホスト名）。

インライン結果（Inline Result）

インライン モードで動作しているときに、侵入イベントをトリガーしたパケットをシステムがドロップした、またはドロップするはずだったか。ブランクは、トリガーとして使用されたルールが [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されていないことを示します

侵入ポリシー（Intrusion Policy）

イベントを生成したルールが有効にされた侵入ポリシー。

IPS ブロックタイプ インジケータ（IPS Blocktype Indicator）

イベントのトラフィック フローと一致する侵入ルールのアクション。

最後のパケット（Last Packet）

セッションの最後のパケットが検出された日時。

MPLSラベル（MPLS Label）

この侵入イベントをトリガーしたパケットと関連付けられているマルチプロトコル ラベル スイッチング ラベル。

マルウェア ブロックタイプ インジケータ（Malware Blocktype Indicator）

イベントのトラフィック フローと一致するファイル ルールで指定されたブロックのタイプ。ブロックまたはインタラクティブ ブロック。

メッセージ（Message）

侵入イベントの場合、イベントの説明テキスト。マルウェアまたはファイル イベントの場合は、マルウェア イベントに関連付けられている追加情報。

NetBIOS ドメイン（NetBIOS Domain）

セッションで使用された NetBIOS ドメイン。

元のクライアントの国と大陸（Original Client Country and Continent）

セッションを開始した元のクライアント ホストの所在地の国と地域の名前。元のクライアントの IP アドレスがルーティング可能であるときにのみ使用できます。

クライアントのオリジナル IP（Original Client IP）

HTTP 接続を開始したクライアントの元の IP アドレス。このアドレスは、X-Forwarded-For（XFF）または True-Client-IP HTTP のヘッダー フィールド、またはそれらの同等品から取得されます。

ポリシー、ポリシーの改訂（Policy、Policy Revision）

アクセス コントロール ポリシーとその改訂版。イベントに関連付けられているアクセス（ファイアウォール）ルールを含みます。

プライオリティ（Priority）

Cisco Talos Security Intelligence and Research Group（Talos）によって決定されたイベント優先順位：High、Medium、または Low。

プロトコル（Protocol）

接続に使用されるトランスポート プロトコルです。

理由（Reason）

次の場合に接続がロギングされた 1 つまたは複数の原因。

理由	説明
ファイル ブロック（File Block）	ファイルまたはマルウェア ファイルが接続に含まれており、システムがその送信を防いでいます。[ファイルブロック（File Block）] の理由は必ず [ブロック（Block）] のアクションと対として組み合わされます。
ファイルモニタ（File Monitor）	システムが接続において特定のファイルの種類を検出しました。
ファイル復帰許可（File Resume Allow）	ファイル送信がはじめに [ファイル ブロック（Block Files）] ルールまたは [マルウェア ブロック（Block Malware）] ファイル ルールによってブロックされました。ファイルを許可する新しいアクセス コントロール ポリシーが展開された後、HTTP セッションが自動的に再開しました。
ファイル復帰ブロック（File Resume Block）	ファイル送信がはじめに [ファイル検出（Detect Files）] ルールまたは [マルウェア クラウド ルックアップ（Malware Cloud Lookup）] ファイル ルールによって許可されました。ファイルをブロックする新しいアクセス コントロール ポリシーが展開された後、HTTP セッションが自動的に停止しました。
侵入ブロック（Intrusion Block）	接続で検出されたエクスプロイト（侵入ポリシー違反）をシステムがブロックしたか、ブロックするはずでした。[侵入ブロック（Intrusion Block）] の原因は、ブロックされたエクスプロイトの場合は [ブロック（Block）]、ブロックされるはずだったエクスプロイトの場合は [許可（Allow）] のアクションと対として組み合わされます。
侵入モニタ（Intrusion Monitor）	接続で検出されたエクスプロイトをシステムが検出したものの、ブロックしなかったことを示します。これは、トリガーされた侵入ルールの状態が [イベントを生成する（Generate Events）] に設定されている場合に発生します。

受信時間（Receive Times）

イベントが生成された日時。

参照ホスト（Referenced Host）

接続のプロトコルが DNS、HTTP、または HTTPS の場合、このフィールドにはそれぞれのプロトコルが使用していたホスト名が表示されます。

レスポンダ バイト、レスポンダ パケット（Responder Bytes、Responder Packets）

セッション レスポンダが送信した合計バイト数またはパケット数。

レスポンダの国または大陸（Responder Country and Continent）

セッションに応答したホストの所在地の国と地域の名前。レスポンダの IP アドレスがルーティング可能であるときにのみ使用できます。

レスポンダ IP（Responder IP）

セッション レスポンダのホスト IP アドレス（および DNS 解決が有効化されている場合はホスト名）。

シグネチャ（Signature）

イベントのトラフィックと一致する侵入ルールのシグネチャ ID。

ソースの国または大陸（Source Country and Continent）

送信元ホストの国および大陸。送信元 IP アドレスがルーティング可能であるときにのみ使用できます。

ソース IP

侵入イベントで送信元ホストが使用する IP アドレス。

送信元ポート/ICMP タイプ、送信元ポート、送信元ポート Itype（Source Port/ICMP Type、Source Port、Source Port Itype）

セッション イニシエータが使用するポートまたは ICMP タイプ。

TCP フラグ（TCP Flags）

接続で検出された TCP フラグ。

URL、URL カテゴリ、URL レピュテーション、URL レピュテーション スコア（URL、URL Category、URL Reputation、URL Reputation Score）

セッション中に監視対象のホストによって要求された URL と、関連付けられたカテゴリ、レピュテーション、およびレピュテーション スコア（利用できる場合）。

システムが SSL アプリケーションを識別またはブロックする場合、要求された URL は暗号化トラフィック内にあるため、システムは、SSL 証明書に基づいてトラフィックを識別します。したがって SSL アプリケーションの場合、この URL は証明書に含まれる一般名を表示します。

ユーザ（User）

イニシエータの IP アドレスに関連付けられたユーザ。

VLAN

イベントをトリガーしたパケットに関連付けられている最内部 VLAN ID。

Web アプリケーションのビジネスとの関連性（Web App Business Relevance）

接続で検出された Web アプリケーション トラフィックに関連するビジネス関連性：Very High、High、Medium、Low、または Very Low。接続で検出された Web アプリケーションのタイプごとに、ビジネスとの関連性が関連付けられています。このフィールドは、最も低いもの（関連性が最も低い）を表示します。

Web アプリケーション カテゴリ、Web アプリケーション タグ（Web App Categories、Web App Tag）

Web アプリケーションの機能を理解するのに役立つ、Web アプリケーションの特性を示す基準。

Web アプリケーションのリスク（Web App Risk）

接続で検出された Web アプリケーション トラフィックに関連するリスク：Very High、High、Medium、Low、または Very Low。接続で検出された Web アプリケーションのタイプごとに、リスクが関連付けられています。このフィールドは、最も高いものを表示します。

Web アプリケーション（Web Application）

接続で検出された HTTP トラフィックの内容または要求された URL を表す Web アプリケーション。

Web アプリケーションがイベントの URL に一致しない場合、そのトラフィックは通常、参照先のトラフィックです（アドバタイズメントのトラフィックなど）。システムは、参照先のトラフィックを検出すると、参照元のアプリケーションを保存し（可能な場合）、そのアプリケーションを Web アプリケーションとして表示します。