侵入イベント

以下のトピックでは、侵入イベントを操作する方法について説明します。

侵入イベントについて

システムは、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する可能性のあるトラフィックがないかどうか、ネットワークをモニターするのに役立ちます。主要なネットワーク セグメントに管理対象デバイスを配置すると、悪意のあるアクティビティを目的としてネットワークを通過するパケットを検査できます。このシステムには、攻撃者が開発したさまざまなエクスプロイトを検索するのに使用できるいくつかのメカニズムがあります。

システムは、潜在的な侵入を特定すると侵入イベント（古い用語で「IPS イベント」と呼ばれることもあります）を生成します。これは、エクスプロイトの日付、時間、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データです。パケットベースのイベントの場合、イベントをトリガーとして使用したパケットのコピーも記録されます。管理対象デバイスは、Secure Firewall Management Center にイベントを送信します。ここで、集約データを確認し、ネットワーク アセットに対する攻撃を的確に把握できます。

管理対象デバイスをインライン、スイッチド、またはルーテッドの侵入システムとして展開することもできます。これにより、危険だと認識したパケットをドロップまたは置換するようデバイスを設定できます。

侵入イベントを確認および評価するためのツール

侵入イベントを検討し、それらがネットワーク環境やセキュリティポリシーの観点から重要かどうかを評価するために、次のツールを使用できます。

- 管理対象デバイスでの現在のアクティビティの概要について説明するイベント要約ページ
- 選択した任意の期間に生成できるテキストベースおよびグラフィカルなレポート。独自のレポートを設計し、スケジュールされた間隔で実行されるよう設定することもできます
- 攻撃に関連したイベントデータの収集に使用できるインシデント処理ツール。調査や応答のトラッキングに役立つ注記を追加することもできます
- SNMP、電子メール、および syslog で設定できる自動アラート
- 特定の侵入イベントに対する応答や修復に使用できる自動化された相関ポリシー
- データをドリルダウンして、さらに調査したいイベントを特定するのに使用できる定義済みカスタムワークフロー
- データを管理および分析するための外部ツール。syslog、eStreamer を使用して、これらのツールにデータを送信できます。詳細については、外部ツールを使用したイベントの分析を参照してください。

また、[分析（Analysis）] > [詳細（Advanced）] > [状況に応じた相互起動（Contextual Cross-Launch）] ページで、事前定義されたリソースなどの公開情報を使用して、悪意のあるエンティティについて詳しく知ることができます。

特定のメッセージ文字列を検索し、イベントを生成したルールのドキュメントを取得するには、https://www.snort.org/rule_docs/ を参照してください。

侵入イベントのライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

侵入イベントの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- 侵入管理者

侵入イベントの表示

侵入イベントは、ネットワーク セキュリティに対する脅威があるかどうかを判断するために表示します。

初期の侵入イベント ビューは、ページにアクセスするために使用するワークフローによって異なります。1 つ以上のドリルダウン ページ、侵入イベントのテーブル ビュー、および終了パケット ビューを含む、定義済みワークフローの 1 つを使用するか、独自のワークフローを作成できます。カスタム テーブルに基づいてワークフローを表示することもできます。これには、侵入イベントを含めることができます。

大量の IP アドレスが含まれている状態で、[IP アドレスの解決（Resolve IP Addresses）] イベント ビュー設定が有効になっていると、イベント ビューの表示が遅くなる場合があります。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[分析（Analysis）] > [侵入（Intrusions）] > [イベント（Events）]**を選択します。

ステップ 2 次の選択肢があります。

- 時間範囲の調整：時間枠の変更の説明に従って、イベント ビューの時間範囲を調整します。
- ワークフローの変更：侵入イベントのテーブル ビューが含まれないカスタム ワークフローを使用している場合、ワークフローのタイトルの横にある [(ワークフローの切り替え)（(switch workflow)）] をクリックして、システム提供のワークフローのいずれかを選択します。
- 制約：表示する対象を分析において重要な侵入イベントに狭めるには、侵入イベント ワークフローの使用 （26 ページ）を参照してください。
- イベントの削除：データベースからイベントを削除するには、[削除（Delete）] をクリックして表示しているパケットのイベントを削除するか、[すべて削除（Delete All）] をクリックして以前に選択したパケットのすべてのイベントを削除します。
- 確認済みのマークを付ける：侵入イベントに確認済みのマークを付けるには、侵入イベントを確認済みとしてマーク （20 ページ）を参照してください。

- 接続データの表示：侵入イベントに関連付けられた接続データを表示するには、侵入イベントに関連付けられた接続データの表示 （20 ページ）を参照してください。
- 内容の表示：侵入イベント フィールド （4 ページ）の説明に従ってテーブルのカラムの内容を表示します。

関連トピック

侵入イベント パケット ビューの使用 （30 ページ）

侵入イベントのフィールドについて

システムは、潜在的な侵入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、時間、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データです。パケットベースのイベントの場合、イベントをトリガーとして使用したパケットのコピーも記録されます。

侵入イベント データは [分析（Analysis）] ト> [侵入（Intrusions）] > [イベント（Events）] で Secure Firewall Management Center Web インターフェイスでに表示できます。または外部ツールを使用して使用状況の syslog メッセージの特定のフィールドからデータをエミットします。Syslog のフィールドは下のリストに示されます。同等の syslog がリストされていないフィールドは、syslog メッセージでは使用可能できません。

侵入イベントを検索するときは、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、どのようにしてイベントを記録したかによって異なることに注意してください。たとえば、復号化されたトラフィックでトリガーされた侵入イベントだけが TLS/SSL 情報を含んでいます。

（注） Secure Firewall Management Center の Web インターフェイスの侵入イベントのテーブル ビューの一部のフィールドはデフォルトで無効になっています。セッション中にフィールドを有効にするには、検索制約を拡張してから、[無効の列（Disabled Columns）] の下の列名をクリックします。

侵入イベント フィールド

[アクセス コントロール ポリシー（Access Control Policy）]（syslog：ACPolicy）

イベントを生成した侵入ルール、プリプロセッサ ルール、またはデコーダ ルールが有効になっている侵入ポリシーに関連付けられているアクセス コントロール ポリシー。

アクセス コントロール ルール（Syslog：AccessControlRuleName）

イベントを生成した侵入ルールを呼び出したアクセス コントロール ルール。[デフォルト アクション（Default Action）] は、ルールが有効化されている侵入ポリシーが特定のアクセス コン

トロールルールに関連付けられておらず、代わりに、アクセスコントロールポリシーのデフォルト アクションとして設定されていることを示しています。

次の場合、このフィールドは空になります（または、syslog メッセージの場合は省略されます）。

- 関連ルール/デフォルトアクションなし：侵入インスペクションは、アクセス制御ルールにもデフォルトアクションにも関連付けられていません。たとえば、システムが適用するルールを決定する前に通過する必要があるパケットを処理するために指定された侵入ポリシーによってパケットが検査された場合が該当します。(このポリシーは、アクセス制御ポリシーの [詳細（Advanced）] タブで指定されます。)
- [関連付けられている接続イベントなし（No associated connection event）]：セッションに記録された接続イベントがデータベースから消去されている場合。たとえば、接続イベントに侵入イベントよりも高いターンオーバーがある場合などです。

[アプリケーション プロトコル（Application Protocol）]（syslog：ApplicationProtocol）

（使用可能な場合）侵入イベントをトリガーとして使用したトラフィックで検出されたホスト間の通信を表す、アプリケーション プロトコル。

アプリケーション プロトコル カテゴリおよびタグ（Application Protocol Category and 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）

侵入イベントをトリガーしたトラフィックで検出されたアプリケーションに関連付けられているリスク。[非常に高い（Very High）]、[高（High）]、[中（Medium）]、[低（Low）]、および[非常に低い（Very Low）]。接続で検出される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。このフィールドは、それらのうち最も高いリスクを表示します。

ビジネスとの関連性（Business Relevance）

侵入イベントをトリガーしたトラフィックで検出されたアプリケーションに関連付けられているビジネスとの関連性。[非常に高い（Very High）]、[高（High）]、[中（Medium）]、[低（Low）]、および[非常に低い（Very Low）]。接続で検出されるアプリケーションのタイプごとに関連するビジネスとの関連性があります。このフィールドは、それらのうち最も低い（関連性が最も低い）ものを表示します。

[分類（Classification）]（syslog：Classification）

イベントを生成したルールが属する分類。

侵入イベント詳細で使用可能な分類値のリストを参照してください。

このフィールドを検索するときは、表示するイベントを生成したルールの分類番号を入力するか、分類名または説明のすべてまたは一部を入力します。また、番号、名前、または説明のコンマ区切りリストを入力することもできます。最後に、カスタム分類を追加した場合、その名前または説明のすべてまたは一部を使用して検索することもできます。

[クライアント（Client）]（syslog：Client）

（使用可能な場合）侵入イベントをトリガーとして使用したトラフィックで検出されたモニター対象のホストで実行されているソフトウェアを表す、クライアント アプリケーション。

クライアント カテゴリおよびタグ（Client Category and 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。

Connection Counter （Syslog のみ）

ある接続と別の同時接続を区別するカウンタ。このフィールドは、それ自体には意味がありません。

[DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、特定の侵入イベントに関連付けられた接続イベントを識別できます。

Connection Instance ID （Syslog のみ）

接続イベントを処理した Snort インスタンス。このフィールドは、それ自体には意味がありません。

[DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、特定の侵入イベントに関連付けられた接続イベントを識別できます。

カウント（Count）

各行に表示される情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません。

CVE ID

このフィールドは検索フィールド専用です。

MITRE の Common Vulnerabilities and Exposures（CVE）データベース（https://cve.mitre.org/）の脆弱性に関連付けられた識別番号による検索。

送信先の大陸（Destination Continent）

侵入イベントに関連する受信ホストの大陸。

送信先の国（Destination Country）

侵入イベントに関連する受信ホストの国。

宛先ホスト重要度（Destination Host Criticality）

イベントが生成されたときの宛先ホスト重要度（対応するホストのホスト重要度属性の値）。

ホストの重要度が変更されても、このフィールドは更新されないことに注意してください。ただし、新しいイベントは新しい重要度の値になります。

[宛先 IP（Destination IP）]（syslog：DstIP）

侵入イベントに関連する受信ホストが使用する IP アドレス。

イニシエータ/レスポンダ、送信元/接続先、および送信者/受信者フィールドに関する注意も参照してください。

[宛先ポート/ICMP コード（Destination Port / ICMP Code）]（syslog：DstPort、ICMPCode）

トラフィックを受信するホストのポート番号。ICMP トラフィックの場合は、ポート番号がないため、このフィールドには ICMP コードが表示されます。

宛先ユーザー（Destination User）

接続イベントのレスポンダー IP に関連付けられたユーザー名。このホストは、エクスプロイトを受信するホストである場合とそうでない場合があります。この値は、通常、ネットワーク上のユーザーだけに知らされます。

。

イニシエータ/レスポンダ、送信元/接続先、および送信者/受信者フィールドに関する注意も参照してください。

デバイス

アクセス コントロール ポリシーが展開された管理対象デバイス。

DeviceUUID （Syslog のみ）

イベントを生成した Firepower デバイスの一意の識別子。

[DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、特定の侵入イベントに関連付けられた接続イベントを識別できます。

ドメイン（Domain）

侵入を検出したデバイスのドメイン。このフィールドは、マルチテナンシーのためにManagement Center を設定したことがある場合に表示されます。

[出力インターフェイス（Egress Interface）]（syslog：EgressInterface）

イベントをトリガーとして使用したパケットの出力インターフェイス。パッシブインターフェイスの場合、このインターフェイスの列には入力されません。

[出力セキュリティ ゾーン（Egress Security Zone）]：（syslog：EgressZone）

イベントをトリガーとして使用したパケットの出力セキュリティ ゾーン。パッシブ展開環境では、このセキュリティ ゾーンのフィールドには入力されません。

[出力仮想ルータ（Egress Virtual Router）]

仮想ルーティングを使用するネットワークでは、トラフィックがネットワークから出るときに通過する仮想ルータの名前。

電子メールの添付ファイル（Email Attachments）

[MIME コンテンツ - 傾向（MIME Content-Disposition）] 見出しから取得された MIME 添付ファイル名。添付ファイルの名前を表示するには、SMTP プリプロセッサの [MIME 添付ファイル名のログ（Log MIME Attachment Names）] オプションを有効にする必要があります。複数の添付ファイル名がサポートされます。

電子メールのヘッダー（Email Headers）

このフィールドは検索フィールド専用です。

電子メールのヘッダーから取得したデータ。

電子メールのヘッダーを SMTP トラフィックの侵入イベントと関連付けるには、SMTP プリプロセッサの [ヘッダーのログ（Log Headers）] オプションを有効にする必要があります。

メール受信者（Email Recipient）

SMTP RCPT TO コマンドから取得された電子メール受信者のアドレス。このフィールドの値を表示するには、SMTP プリプロセッサの [受信者アドレスのログ（Log To Addresses）] オプションを有効にする必要があります。複数の受信者アドレスがサポートされます。

メール送信者（Email Sender）

SMTP MAIL FROM コマンドから取得された電子メール送信者のアドレス。このフィールドの値を表示するには、SMTP プリプロセッサの [送信者アドレスのログ（Log From Address）] オプションを有効にする必要があります。複数の送信者アドレスがサポートされます。

First Packet Time （Syslog のみ）

システムが最初のパケットを検出した時間。

[DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、特定の侵入イベントに関連付けられた接続イベントを識別できます。

ジェネレータ（Generator）

イベントを生成したコンポーネント。

次の侵入イベント フィールドに関する情報も参照してください。[GID]、[メッセージ（Message）]、および [Snort ID]

GID（syslog のみ）

ジェネレータ ID。イベントを生成したコンポーネントの ID。

次の侵入イベントフィールドに関する情報も参照してください。[ジェネレータ（Generator）]、[メッセージ（Message）]、および [Snort ID]

HTTP ホスト名（HTTP Hostname）

HTTP 要求のホスト見出しから取得されたホスト名（存在する場合）。要求パケットにホスト名が常に含まれているわけではないことに注意してください。

ホスト名を HTTP クライアント トラフィックの侵入イベントと関連付けるには、HTTP 検査プリプロセッサの [ホスト名のログ（Log Headers）] オプションを有効にする必要があります。

テーブル ビューで、この列には、取得されたホスト名の最初の 50 文字が表示されます。ホストの省略名の表示部分にポインタを合わせると、最大256バイトまでの完全な名前を表示することができます。また、最大256バイトまでの完全なホスト名をパケット ビューに表示することもできます。

[HTTP 応答コード（HTTP Response Code）]（syslog：HTTPResponse）

イベントをトリガーした接続を介してクライアントの HTTP 要求に応答して送信される HTTP ステータス コード。

HTTP URI

（存在する場合）侵入イベントをトリガーとして使用したHTTP要求パケットに関連付けられた raw URI。要求パケットに URI が常に含まれているわけではないことに注意してください。

URI を HTTP クライアント トラフィックの侵入イベントと関連付けるには、HTTP 検査プリプロセッサの [URI のログ（Log URI）] オプションを有効にする必要があります。

HTTP応答によってトリガーとして使用された侵入イベントの関連HTTP URIを参照するには、[両方のポートでのストリーム再構成の実行（Perform Stream Reassembly on Both Ports）] オプションにHTTPサーバのポートを設定する必要があります。ただし、これにより、トラフィックのリアセンブル用のリソース要求が増加することに注意してください。

この列には、取得された URI の最初の 50 文字が表示されます。省略 URI の表示部分にポインタを合わせると、最大 2048 バイトまでの完全な URI を表示することができます。また、最大 2048 バイトまでの完全な URI をパケット ビューに表示することもできます。

影響（Impact）

このフィールドの影響レベルは、侵入データ、ネットワーク検出データ、脆弱性情報との関係を示します。

このフィールドを検索するときは、影響アイコンの色または一部の文字列を指定しないでください。たとえば、**blue**、**level 1**、または **0** を使用しないでください。有効な大文字と小文字を区別しない値は次のとおりです。

- Impact 0、Impact Level 0
- Impact 1、Impact Level 1
- Impact 2、Impact Level 2
- Impact 3、Impact Level 3
- Impact 4、Impact Level 4

NetFlow データからネットワークマップに追加されたホストに使用可能なオペレーティングシステムの情報はないので、システムは、それらのホストに作用する侵入イベントに対し脆弱な（インパクト レベル 1：赤）インパクトレベルを割り当てることができません。このような場合は、ホスト入力機能を使用して、ホストのオペレーティングシステム ID を手動で設定します。

入力インターフェイス (Syslog：IngressInterface)

イベントをトリガーとして使用したパケットの入力インターフェイス。パッシブ インターフェイスの場合、このインターフェイスの列だけに入力されます。

[入力セキュリティ ゾーン（Ingress Security Zone）]：（syslog：IngressZone）

イベントをトリガーとして使用したパケットの入力セキュリティ ゾーンまたはトンネル ゾーン。パッシブ展開環境では、このセキュリティ ゾーン フィールドだけに入力されます。

[入力仮想ルータ（Ingress Virtual Router）]

仮想ルーティングを使用するネットワークでは、トラフィックがネットワークに入るときに通過する仮想ルータの名前。

[インライン結果（Inline Result）]（syslog：InlineResult）

ワークフローとテーブル ビューでは、このフィールドには次のいずれかが表示されます。

表 *1:* ワークフロー ビューとテーブル ビューの *[*インライン結果（*Inline Result*）*]* フィールドの内容

アイコン	意味
	ルールをトリガーしたパケットをシステムがドロップしました。
	[インライン時にドロップ（Drop when Inline）] 侵入ポリシーオプション（インライン展開環境）を有効にした場合、またはシステムがプルーニングしている間に [ドロップしてイベントを生成する（Drop and Generate）] ルールがイベントを生成した場合、IPS がパケットをドロップしたことを示します。

アイコン	意味
	IPS はパケットを宛先に送信または配信した可能性がありますが、このパケットを含む接続は現在ブロックされています。
アイコンなし（空白）	トリガーされたルールは [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されていませんでした

次の表に、インライン結果の考えられる理由の一覧を示します（「would have dropped」および「partially dropped」）。

インライン結果	理由	詳細な理由
would have dropped	パッシブモードまたはタップモードのインターフェイス	インラインのタップモードまたはパッシブモードでインターフェイスを構成しています。
	「検出」検査モードの侵入ポリシー	侵入ポリシーの検査モードを検出に設定しています。
	接続のタイムアウト	TCP/IP 接続がタイムアウトしたため、Snort 検査エンジンは検査を一時停止しました。
partially dropped	接続が終了しました（0x01）	新しいフローの作成中に、割り当てられたフローが許可されたフロー数を超える場合、Snort 検査エンジンは、最も使用頻度の低いフローをプルーニングします。
	接続が終了しました（0x02）	Snort 検査エンジンを再読み込みすると、メモリが調整され、エンジンは最も使用頻度の低いフローをプルーニングします。
	接続が終了しました（0x04）	Snort 検査エンジンが正常にシャットダウンすると、エンジンはすべてのアクティブなフローをパージします。

パッシブ展開では、侵入ポリシーのルールの状態やインライン ドロップ動作に関係なく、インライン インターフェイスがタップ モードの場合を含めて、システムはパケットをドロップしません。

このフィールドを検索するときは、次のいずれかを入力します。

- **dropped**：インライン展開環境でパケットをドロップするかどうかを指定します。
- **would have dropped**：インライン展開環境でパケットをドロップするように侵入ポリシーが設定されている場合に、パケットをドロップするかどうかを指定します。
- **partially dropped**：パケットが宛先に送信または配信されるかどうかを指定します。ただし、このパケットを含む接続は現在ブロックされています。

侵入ポリシー (Syslog: IntrusionPolicy)

イベントを生成した侵入ルール、プリプロセッサ ルール、またはデコーダ ルールが有効にされた侵入ポリシー。アクセス コントロール ポリシーのデフォルト アクションとして侵入ポリシーを選択するか、アクセス コントロール ルールと侵入ポリシーを関連付けることができます。

IOC（syslog：NumIOC）

侵入イベントをトリガーとして使用したトラフィックが、接続に関係するホストに対する侵入の痕跡（IOC）もトリガーとして使用したかどうか。

このフィールドを検索するときは、**triggered** または **n/a** を指定します。

[メッセージ（Message）]（syslog：メッセージ）

イベントを説明するテキスト。ルールベースの侵入イベントの場合、イベント メッセージはルールから取得されます。デコーダベースおよびプリプロセッサベースのイベントの場合は、イベント メッセージはハード コーディングされています。

ジェネレータおよび Snort ID（GID と SID）と SID バージョン（改訂）はカッコで囲んだコロン区切りの数字形式で各メッセージの末尾に付加されます（GID:SID:version）。例：**(1:36330:2)**。

MITRE

クリックしてモーダルを起動できる技術の数。これは、その階層内にある MITRE の戦術と技術の全リストを示します。

[MPLS ラベル（MPLS Label）]（syslog：MPLS_Label）

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。

[ネットワーク分析ポリシー（Network Analysis Policy）]（syslog：NAPPolicy）

イベントの生成に関連付けられているネットワーク分析ポリシー（ある場合）。

このフィールドには、取得された URI の最初の 50 文字が表示されます。省略 URI の表示部分にポインタを合わせると、最大 2048 バイトまでの完全な URI を表示することができます。また、最大 2048 バイトまでの完全な URI をパケット ビューに表示することもできます。

クライアントのオリジナル IP（Original Client IP）

X-Forwarded-For（XFF）、True-Client-IP、またはカスタム定義の HTTP ヘッダーから取得された、元のクライアント IP アドレス。

このフィールドの値を表示するには、ネットワーク解析ポリシーで HTTP プリプロセッサ [元のクライアント IP アドレスの抽出（Extract Original Client IP Address）] オプションを有効にする必要があります。オプションで、ネットワーク解析ポリシーの同じエリアで、最大 6 つのカスタム クライアント IP 見出しを指定し、システムが [クライアントのオリジナル IP（Original Client IP）] イベント フィールドの値を選択する優先順位を設定します。

[優先度（Priority）]（syslog：Priority）

Talos インテリジェンスグループ で指定されたイベントの優先度。優先度は、`priority` キーワードの値または `classtype` キーワードの値に対応します。その他の侵入イベントの場合、プライオリティはデコーダまたはプリプロセッサによって決定されます。有効な値は、[高（high）]、[中（medium）]、および [低（low）] です。

[プロトコル（Protocol）]（syslog：Protocol）

Secure Firewall Management Center の Web インターフェイスでは、このフィールドは検索フィールド専用です。

http://www.iana.org/assignments/protocol-numbers に一覧表示されている、接続で使用するトランスポート プロトコルの名前または番号。これは、送信元および宛先ポート/ICMP の列と関連付けられたプロトコルです。

確認者（Reviewed By）

イベントを確認したユーザの名前。このフィールドを検索するときは、**`unreviewed`** と入力すると、まだ確認されていないイベントを検索できます。

Revision（syslog のみ）

イベントの生成に使用された署名のバージョン。

次の侵入イベント フィールドに関する情報も参照してください。[ジェネレータ（Generator）]、[GID]、[メッセージ（Message）]、[SID]、および [Snort ID]

ルールグループ

クリックしてモーダルを起動できる非 MITRE ルールグループの数。これは、ルールグループの全リストを示します。

[セキュリティ コンテキスト（Security Context）]（syslog：Context）

トラフィックが通過した仮想ファイアウォール グループを識別するメタデータ。システムがこのフィールドにデータを設定するのは、マルチコンテキストモードの ASA FirePOWER だけです。

SID（syslog のみ）

イベントを生成したルールの署名 ID（Snort ID ともいう）

次の侵入イベントフィールドに関する情報も参照してください。[ジェネレータ（Generator）]、[GID]、[メッセージ（Message）]、[改訂（Revision）]、および [Snort ID]

Snort ID

このフィールドは検索フィールド専用です。

（syslog フィールドについては、SID を参照してください。）

検索を実行する場合：イベントを生成したルールの（[Snort ID]SID）を指定するか、オプションで、ルールの複合ジェネレータ ID（GID）および SID を指定します。ここで、GID および SID はコロン（:）で区切られ、GID:SID の形式になります。次の表の任意の値を指定できます。

表 *2 : [Snort ID]* 検索値

値	例
単一の SID	10000
SID の範囲	10000-11000
SID より大きい	>10000
SID 以上	>=10000
SID 未満	<10000
SID 以下	<=10000
SID のカンマ区切りリスト	10000,11000,12000
単一の GID:SID の組み合わせ	1:10000
GID:SID の組み合わせのカンマ区切りリスト	1:10000,1:11000,1:12000
SID および GID:SID の組み合わせのカンマ区切りリスト	10000,1:11000,12000

表示しているイベントの SID が [メッセージ（Message）] 列に表示されます。詳細については、この項の [メッセージ（Message）] フィールドについての説明を参照してください。

ソースの大陸（Source Continent）

侵入イベントに関連する送信ホストのある大陸。

ソースの国（Source Country）

侵入イベントに関連する送信ホストのある国。

送信元ホスト重要度（Source Host Criticality）

イベントが生成されたときの送信元ホスト重要度（対応するホストのホスト重要度属性の値）。

ホストの重要度が変更されても、このフィールドは更新されないことに注意してください。ただし、新しいイベントは新しい重要度の値になります。

[送信元 IP（Source IP）]（syslog：SrcIP）

侵入イベントに関連する送信ホストが使用する IP アドレス。

イニシエータ/レスポンダ、送信元/接続先、および送信者/受信者フィールドに関する注意も参照してください。

[送信元ポート/ICMP タイプ（Source Port/ICMP Type）]（syslog：SrcPort、ICMPType）

送信元ホストのポート番号。ICMP トラフィックの場合は、ポート番号がないため、このフィールドには ICMP タイプが表示されます。

[送信元ユーザー（Source User）]（syslog：User）

接続を開始したホストの IP アドレスに関連付けられたユーザー名。エクスプロイトの送信元ホストである場合とそうでない場合があります。このユーザー値は、通常、ネットワーク上のユーザーだけに知らされます。

該当する場合、ユーザー名の前には `<realm>\` が付いています。

SSL Actual Action (Syslog: SSLActualAction)

Secure Firewall Management Center の Web インターフェイスでは、このフィールドは検索フィールド専用です。

システムが暗号化されたトラフィックに適用したアクション。

ブロック/リセット付きブロック（Block/Block with reset）

ブロックされた暗号化接続を表します。

[復号（再署名）（Decrypt (Resign)）]

再署名サーバ証明書を使用して復号された発信接続を表します。

[復号（キーの交換）（Decrypt (Replace Key)）]

置き換えられた公開キーと自己署名サーバ証明書を使用して復号化された発信接続を表します。

[復号（既知のキー）（Decrypt (Known Key)）]

既知の秘密キーを使用して復号化された着信接続を表します。

[デフォルトアクション（Default Action）]

接続がデフォルト アクションによって処理されたことを示します。

[復号しない（Do not Decrypt）]

システムが復号化しなかった接続を表します。

フィールド値は、検索ワークフロー ページの [SSL ステータス（SSL Status）] フィールドに表示されます。

[SSL 証明書情報（SSL Certificate Information）]

このフィールドは検索フィールド専用です。

トラフィックを暗号化するための公開キー証明書に保存される次の情報：

- サブジェクト/発行元共通名（Subject/Issuer Common Name）
- サブジェクト/発行元組織（Subject/Issuer Organization）
- サブジェクト/発行元組織単位（Subject/Issuer Organization Unit）
- 有効期間の開始/終了（Not Valid Before/After）
- シリアル番号（Serial Number）
- 証明書フィンガープリント（Certificate Fingerprint）
- 公開キー フィンガープリント（Public Key Fingerprint）

SSL 失敗理由（SSL Failure Reason）

このフィールドは検索フィールド専用です。

システムが暗号化されたトラフィックの復号化に失敗した理由。

- 不明
- 不一致（No Match）
- Success
- キャッシュされていないセッション（Uncached Session）
- 不明な暗号スイート（Unknown Cipher Suite）
- サポートされていない暗号スイート（Unsupported Cipher Suite）
- サポートされていない SSL バージョン（Unsupported SSL Version）
- 使用された SSL 圧縮（SSL Compression Used）
- パッシブ モードで復号化できないセッション（Session Undecryptable in Passive Mode）
- ハンドシェイク エラー（Handshake Error）
- 復号エラー（Decryption Error）
- 保留中のサーバー名カテゴリの検索（Pending Server Name Category Lookup）

- 保留中の共通名カテゴリの検索（Pending Common Name Category Lookup）
- 内部エラー（Internal Error）
- 使用不可能なネットワーク パラメータ（Network Parameters Unavailable）
- 無効なサーバー証明書の処理（Invalid Server Certificate Handle）
- 使用不可能なサーバー証明書フィンガープリント（Server Certificate Fingerprint Unavailable）
- サブジェクト DN をキャッシュできない（Cannot Cache Subject DN）
- 発行元 DN をキャッシュできない（Cannot Cache Issuer DN）
- 不明な SSL バージョン（Unknown SSL Version）
- 使用不可能な外部証明書リスト（External Certificate List Unavailable）
- 使用不可能な外部証明書フィンガープリント（External Certificate Fingerprint Unavailable）
- 無効な内部証明書リスト（Internal Certificate List Invalid）
- 使用不可能な内部証明書リスト（Internal Certificate List Unavailable）
- 使用不可能な内部証明書（Internal Certificate Unavailable）
- 使用不可能な内部証明書フィンガープリント（Internal Certificate Fingerprint Unavailable）
- 使用不可能なサーバー証明書の検証（Server Certificate Validation Unavailable）
- サーバー証明書の検証エラー（Server Certificate Validation Failure）
- 無効なアクション（Invalid Action）

フィールド値は、検索ワークフロー ページの [SSL ステータス（SSL Status）] フィールドに表示されます。

SSL ステータス（SSL Status）

暗号化された接続を記録した、[SSLの実際の動作（SSL Actual Action）]（復号ルール、デフォルトアクション、または復号できないトラフィックアクション）に関連したアクション。

システムが暗号化された接続の復号化に失敗した場合、実行された [SSL の実際のアクション（SSL Actual Action）]（復号化できないトラフィック アクション）と [SSL 障害の理由（SSL Failure Reason）] が表示されます。たとえば、不明な暗号スイートによって暗号化されたトラフィックをシステムが検出し、それ以上のインスペクションをせずにこれを許可した場合、このフィールドには [復号しない（不明な暗号スイート）（Do Not Decrypt (Unknown Cipher Suite)）] が表示されます。

証明書の詳細を表示するには [ロック（Lock）] アイコン（）をクリックします。

このフィールドを検索するときは、[SSL の実際のアクション（SSL Actual Action）] および [SSL 障害の理由（SSL Failure Reason）] の値を 1 つ以上を入力して、システムが処理した暗号化されたトラフィック、または復号化に失敗したトラフィックを表示します。

[SSL サブジェクト/発行元国（SSL Subject/Issuer Country）]

このフィールドは検索フィールド専用です。

暗号化証明書に関連付けられている件名または発行者の国に関する 2 文字の ISO 3166-1 アルファ 2 国コード。

時刻（Time）

イベントの日付と時刻。このフィールドは検索できません。

[VLAN ID]（syslog：VLAN_ID）

侵入イベントをトリガーとして使用したパケットと関連付けられた最内部 VLAN ID。

[Web アプリケーション（Web Application）]（syslog：WebApplication）

侵入イベントをトリガーとして使用したトラフィックで検出された 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。

システムが HTTP のアプリケーション プロトコルを検出し、特定の Web アプリケーションを検出できなかった場合、システムは代わりに一般的な Web ブラウジング指定を提供します。

Web アプリケーション カテゴリおよびタグ（Web Application Category and 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。

関連トピック

イベントの検索

侵入イベント影響レベル

イベントがネットワークに与える影響を評価するために、Secure Firewall Management Center は侵入イベントのテーブル ビューに影響レベルを表示します。イベントごとに、システムは影響レベル アイコンを追加し、侵入データ、ネットワーク検出データ、脆弱性情報との関係を色で示します。

（注） NetFlow データからネットワークマップに追加されたホストに使用可能なオペレーティングシステムの情報はないので、システムは、それらのホストに作用する侵入イベントに対し脆弱な（インパクト レベル 1：赤）インパクトレベルを割り当てることができません。このような場合は、ホスト入力機能を使用して、ホストのオペレーティングシステム ID を手動で設定します。

次の表に、影響レベルで使用可能な値を示します。

表 *3*: 影響レベル

影響レベル	脆弱性	カラー	説明
[不明（Unknown）]（0）	不明	グレー	送信元ホストと宛先ホストは両方ともネットワーク検出によってモニタされているネットワーク上に存在しません。
[脆弱（Vulnerable）]（1）	脆弱	赤色	次のいずれかを行います。 • 送信元ホストまたは宛先ホストはネットワークマップ内にあり、脆弱性はホストにマッピングされます • 送信元ホストまたは宛先ホストは、ウイルス、トロイの木馬、または他の悪意のあるソフトウェアによって侵害される可能性があります。
[潜在的に脆弱（Potentially Vulnerable）]（2）	潜在的に脆弱	オレンジ	送信元ホストまたは宛先ホストはネットワークマップ内にあり、次のいずれかに当てはまります。 • ポート指向のトラフィックの場合、ポートはサーバアプリケーションプロトコルを実行しています • ポート指向ではないトラフィックの場合、ホストはプロトコルを使用します
[現在脆弱性のない（Currently Not Vulnerable）]（3）	現在は脆弱ではない	黄色	送信元ホストまたは宛先ホストはネットワークマップ内にあり、次のいずれかに当てはまります。 • ポート指向のトラフィック（たとえば、TCPまたはUDP）の場合、ポートが開いていません • ポート指向ではないトラフィック（たとえば、ICMP）の場合、ホストはプロトコルを使用しません
[不明なターゲット（Unknown Target）]（4）	不明なターゲット	青	送信元ホストまたは宛先ホストがモニター対象のネットワークにありますが、ネットワークマップ内にそのホストのエントリがありません。

侵入イベントに関連付けられた接続データの表示

システムは、侵入イベントが検出された接続を記録できます。このロギングは、アクセス コントロール ルールに関連付けられている侵入ポリシーに対して自動的に行われますが、デフォルト アクションに関連する接続データを参照するには、接続ロギングを手動で有効にする必要があります。

関連データの表示は、イベントのテーブル ビュー間を移動する場合に非常に役立ちます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[分析（Analysis）] > [侵入（Intrusions）] > [イベント（Events）]**を選択します。

ステップ 2 テーブルのチェックボックスを使用して侵入イベントを選択してから、[ジャンプ（Jump to）] ドロップダウン リストから [接続（Connections）] を選択します。

ヒント 同じ方法で、特定の接続に関連した侵入イベントを表示できます。詳細については、ワークフロー間のナビゲーションを参照してください。

関連トピック

許可された接続のロギング
侵入イベント ワークフローの使用 （26 ページ）
接続およびセキュリティ関連の接続イベントテーブルの使用

侵入イベントを確認済みとしてマーク

侵入イベントが悪意のあるものではないことがわかったら、そのイベントを確認済みとしてマークできます。

侵入イベントを調べて、そのイベントがネットワーク セキュリティに対して脅威ではないことがわかったら（たとえば、ネットワーク上のどのホストも検出されたエクスプロイトに対して脆弱でないことがわかっているなど）、そのイベントを確認済みとしてマークできます。確認済みのイベントはイベント データベースに保存され、イベント要約統計に含まれますが、デフォルトの侵入イベント ページには表示されなくなります。自分の名前がレビューアとして表示されます。

マルチドメイン展開では、イベントに確認済みのマークを付けると、そのイベントを表示可能なすべてのドメインでシステムによってイベントに確認済みのマークが付けられます。

バックアップを実行してから確認済みの侵入イベント ビューを削除した場合、バックアップを復元すると、削除された侵入イベント ビューは復元されますが、確認済みのステータスは復元されません。こうして復元された侵入イベントは、[確認済みイベント（Reviewed Events）] の下ではなく [侵入イベント（Intrusion Events）] の下に表示されます。

手順

侵入イベントが表示されるページで、次の 2 つの方法を選択できます。

- イベントのリストから 1 つまたは複数の侵入イベントにマークを付けるには、イベントの横にあるチェックボックスをオンにして、[レビュー（Review）] をクリックします。
- イベントのリストからすべての侵入イベントにマークを付けるには、[すべて確認（Review All）] をクリックします。

関連トピック

侵入イベント ワークフローの使用 （26 ページ）

以前に確認した侵入イベントの表示

マルチドメイン展開では、イベントに確認済みのマークを付けると、そのイベントを表示可能なすべてのドメインでシステムによってイベントに確認済みのマークが付けられます。

手順

ステップ 1 **[分析（Analysis）] > [侵入（Intrusions）] > [確認済みイベント（Reviewed Events）]**を選択します。

ステップ 2 次の選択肢があります。

- 時間枠の変更の説明に従って、時間範囲を調整します。
- 侵入イベントのテーブル ビューが含まれないカスタム ワークフローを使用している場合、ワークフローのタイトルの横にある [(ワークフローの切り替え)（(switch workflow)）] をクリックして、システム提供のワークフローのいずれかを選択します。
- 表示されるイベントの詳細については、侵入イベント フィールド （4 ページ）を参照してください。

関連トピック

侵入イベント ワークフローの使用 （26 ページ）

確認済み侵入イベントに未確認のマークを付ける

イベントに未確認のマークを付けることで、確認済みイベントをデフォルトの侵入イベント ビューに戻すことができます。

マルチドメイン展開では、イベントに確認済みのマークを付けると、そのイベントを表示可能なすべてのドメインでシステムによってイベントに確認済みのマークが付けられます。

手順

確認済みイベントが表示されるページで、次の 2 つの方法を選択できます。

- 確認済みイベント リストから個別の侵入イベントを削除するには、特定のイベントの横にあるチェックボックスをオンにして、[未確認（Unreview）] をクリックします。
- 確認済みイベント リストからすべての侵入イベントを削除するには、[すべて未確認（Unreview All）] をクリックします。

プリプロセッサ イベント

プリプロセッサが提供する機能は2つあります。1つは、パケットに対して指定されたアクション（HTTP トラフィックを復号して正規化するなど）を実行する機能、もう 1 つは、パケットが特定のプリプロセッサ オプションをトリガーしたときに関連するプリプロセッサ ルールが有効にされている場合は常にイベントを生成することで、指定のプリプロセッサ オプションの実行を報告するという機能です。たとえば、プリプロセッサが IIS の二重にエンコードされたトラフィックを検出した場合にイベントが生成されるようにするには、HTTP Inspect の [二重エンコード（Double Encoding）] オプションと、HTTP Inspect Generator（GID）119 および [Snort ID]（SID）2 が設定された関連するプリプロセッサ ルールを有効にします。

プリプロセッサの実行を報告するイベントを生成すると、異常なプロトコルエクスプロイトを検出するのに役立ちます。たとえば、攻撃者は重複している IP フラグメントを作成して、ホスト上で DoS 攻撃を仕掛ける可能性があります。IP 最適化プリプロセッサはこのタイプの攻撃を検出し、それに関する侵入イベントを生成できます。

プリプロセッサ イベントは、パケット ディスプレイにイベントの詳細なルールの説明が表示されないという点で、ルール イベントとは異なります。代わりに、パケット ディスプレイには、イベント メッセージ、GID、SID、パケット ヘッダー データおよびパケット ペイロードが表示されます。これにより、パケットのヘッダー情報を分析し、そのヘッダー オプションが使用中であるかをどうか判断して、それがシステムをエクスプロイトする可能性がある場合は、パケット ペイロードを検査できます。プリプロセッサによる各パケットの分析が完了すると、ルール エンジンは、その結果に応じて適切なルールを実行し（プリプロセッサが各パケットを最適化し、有効なセッションの一部として確立できた場合）、潜在的なコンテンツ レベルの脅威についてさらに分析を行い、それらのパケットについて報告します。

プリプロセッサのジェネレータ ID

各プリプロセッサには、独自のジェネレータ ID 番号（GID）があり、これはパケットによってトリガーとして使用されたプリプロセッサを示します。一部のプリプロセッサは関連した SID もあり、これは潜在的攻撃を分類する ID 番号です。ルールの [Snort ID]（SID）が、ルールをトリガーとして使用するパケットのコンテキストを提供できる方法とほぼ同じで、この ID 番号によりイベントのタイプを分類することによって、イベントをより効率的に分析するのに役立ちます。侵入ポリシー ルールのページのプリプロセッサ フィルター グループのプリプロセッサごとにプリプロセッサ ルールをリストできます。また、プリプロセッサのプリプロ

セッサ ルールとカテゴリ フィルター グループのパケット デコーダ サブグループをリストできます。

（注） 標準テキスト ルールによって生成されるイベントは、ジェネレータ ID が 1（グローバル ドメインまたはレガシー GID）または 1000 ～ 2000（子孫ドメイン）です。共有オブジェクト ルールの場合、イベントのジェネレータ ID は 3 です。どちらの場合も、トリガーした特定のルールがイベントの SID に示されます。

次の表では、各 GID を生成するイベントのタイプについて説明します。

表 *4*: ジェネレータ *ID*

ID	コンポーネント	説明
1	標準的なテキストルール	パケットが標準テキスト ルールをトリガーとして使用したときにイベントが生成されました（グローバル ドメインまたはレガシー GID）。
2	タグ付きパケット	タグ付きセッションからパケットを生成するタグ ジェネレータによって、イベントが生成されました。これは、`tag`ルール オプションが使用される場合に発生します。
3	共有オブジェクト ルール	パケットが共有オブジェクト ルールをトリガーとして使用したときにイベントが生成されました。
102	HTTP デコーダ	デコーダ エンジンが、パケット内の HTTP データを復号化しました。
105	Back Orifice ディテクタ	Back Orifice ディテクタが、パケットに関連付けられた Back Orifice 攻撃を特定しました。
106	RPC デコーダ	RPC デコーダがパケットを復号化しました。
116	パケット デコーダ	パケット デコーダによってイベントが生成されました。
119、120	HTTP Inspect プリプロセッサ	HTTP Inspect プリプロセッサによってイベントが生成されました。GID 120 ルールは、サーバ固有の HTTP トラフィックに関するルールです。
122	ポートスキャンディテクタ	ポートスキャン フロー ディテクタによってイベントが生成されました。
123	IP デフラグメンタ	断片化された IP データグラムを適切に再構成できなかったときに、イベントが生成されました。
124	SMTP デコーダ	SMTP プリプロセッサが SMTP バーブに対するエクスプロイトを検出したときに、イベントが生成されました。
125	FTP デコーダ	FTP/Telnet デコーダが FTP トラフィック内でエクスプロイトを検出したときに、イベントが生成されました。

ID	コンポーネント	説明
126	Telnet デコーダ	FTP/Telnet デコーダが Telnet トラフィック内でエクスプロイトを検出したときに、イベントが生成されました。
128	SSH プリプロセッサ	SSH プリプロセッサが SSH トラフィック内でエクスプロイトを検出したときに、イベントが生成されました。
129	ストリームプリプロセッサ	ストリーム プリプロセッサによるストリームの前処理中に、イベントが生成されました。
131	DNSプリプロセッサ	DNS プリプロセッサによってイベントが生成されました。
133	DCE/RPC プリプロセッサ	このイベントは、DCE/RPC プリプロセッサにより生成されました。
134	ルール遅延 パケット遅延	ルール遅延によって侵入ルールのグループが中断された（134:1）または再有効化された（134:2）とき、あるいはパケット遅延しきい値が超過したために、システムがパケットの検査を停止したとき（134:3）に、イベントが生成されました。
135	レートベースの攻撃ディテクタ	レートベースの攻撃ディテクタがネットワークのホストに対する過度の識別したときに、イベントが生成されました。
137	SSL プリプロセッサ	TLS/SSL プリプロセッサによってイベントが生成されました。
138、139	機密データプリプロセッサ	機密データ プリプロセッサによってイベントが生成されました。
140	SIP プリプロセッサ	SIP プリプロセッサによってイベントが生成されました。
141	IMAP プリプロセッサ	IMAP プリプロセッサによってイベントが生成されました。
142	POP プリプロセッサ	POP プリプロセッサによってイベントが生成されました。
143	GTP プリプロセッサ	GTP プリプロセッサによってイベントが生成されました。
144	Modbus プリプロセッサ	Modbus SCADA プリプロセッサによってイベントが生成されました。
145	DNP3 プリプロセッサ	DNP3 SCADA プリプロセッサによってイベントが生成されました。
148	CIP プリプロセッサ	CIP SCADA プリプロセッサによってイベントが生成されました。
149	S7Commplus プリプロセッサ	S7Commplus SCADA プリプロセッサによってイベントが生成されました。
1000～2000	標準的なテキストルール	パケットが標準テキスト ルールをトリガーとして使用したときにイベントが生成されました（子孫ドメイン）。

侵入イベントのワークフロー ページ

現在の侵入ポリシーで有効になっているプリプロセッサ、デコーダ、および侵入ルールは、モニタしているトラフィックがポリシーに違反するたびに、侵入イベントを生成します。

システムは、侵入イベントの表示および分析に使用できる、イベントデータが入力された定義済みワークフローのセットを提供します。これらのワークフローは、評価する侵入イベントの特定に役立つ一連のページを表示して手順を示します。

定義済みの侵入イベントのワークフローには、次の3種類のページまたはイベントビューがあります。

- 1つ以上のドリルダウン ページ
- 侵入イベントのテーブル ビュー
- パケット ビュー

ドリルダウン ページには通常、1つの特定の種類の情報を表示できるように1つのテーブル（一部のドリルダウン ビューでは複数のテーブル）に2つ以上の列が含まれます。

「ドリルダウン」して1つ以上の宛先ポートの詳細情報を検索すると、これらのイベントは自動的に選択され、ワークフローの次のページが表示されます。このように、ドリルダウンテーブルを使用すると、一度に分析するイベントの数を減らすことができます。

侵入イベントの最初のテーブル ビューでは、各侵入イベントが独自の行にリストされます。テーブルの列には、時間、発信元IPアドレスおよびポート、宛先IPアドレスおよびポート、イベントの優先度、イベント メッセージなどの情報が示されます。

イベントを選択してワークフローの次のページを表示する代わりに、テーブル ビューでイベントを選択した場合、イベントはいわゆる制約に追加されます。制約とは、分析するイベントの種類に加える制限のことです。

たとえば、任意の列で[閉じる（Close）]（✕）をクリックして、ドロップダウンリストから[時間（Time）]をクリアすると、[時間（Time）]を列の1つとして削除できます。分析内でイベントのリストを絞り込むには、テーブル ビューの行のいずれかの値のリンクをクリックします。たとえば、分析を送信元IPアドレスの1つ（おそらく、潜在的な攻撃者）から生成されたイベントに制限するには、[送信元IPアドレス（Source IP Address）]列のIPアドレスをクリックします。

テーブル ビューの1つまたは複数の行を選択し、[表示（View）]をクリックすると、パケット ビューが表示されます。パケット ビューは、ルールをトリガーとして使用したパケットまたはイベントを生成したプリプロセッサに関する情報を提供します。パケット ビューの各セクションには、パケット内の特定の層についての情報が含まれます。折りたたまれたセクションを展開すると、より多くの情報を参照できます。

（注） それぞれのポートスキャン イベントは複数のパケットによってトリガーとして使用されるため、ポートスキャン イベントは特別なバージョンのパケット ビューを使用します。

事前定義済みのワークフローが特定のニーズに合致しない場合は、必要な情報だけを表示するカスタム ワークフローを作成できます。カスタム侵入イベントのワークフローには、ドリルダウン ページ、イベントのテーブル ビュー、またはその両方を含めることができます。システムはパケット ビューを最後のページとして自動的に組み込みます。イベントを調査する方法に応じて、定義済みワークフローと独自のカスタム ワークフローを簡単に切り替えることができます。

侵入イベント ワークフローの使用

イベントのドリルダウン ビューとテーブル ビューは、イベントのリストを絞り込み、関連するイベントのグループに分析を集中するために使用できる共通機能を共有します。

別のワークフローページで同じ侵入イベントを表示しないようにするため、ページの下部にあるリンクをクリックして別のページのイベントを表示すると時間範囲は一時停止し、クリックして後続のページでその他のアクションを実行すると再開します。

ヒント プロセスの任意の時点で、制約を検索条件のセットとして保存できます。たとえば、ネットワークが数日にわたり単一の IP アドレスから攻撃者によって探られていることに気付いた場合、調査中に制約をいったん保存し、後で使用することができます。ただし、複合制約を検索条件のセットとして保存することはできません。

手順

ステップ 1 **[分析（Analysis）]>[侵入（Intrusions）]>[イベント（Events）]** を使用して侵入イベント ワークフローにアクセスします。

ステップ 2 オプションで、侵入イベント ドリルダウン ページの制約 （28 ページ）または侵入イベント テーブル ビューの制約 （29 ページ）の説明に従って、イベント ビューに表示される侵入イベントの数を制限します。

ステップ 3 次の選択肢があります。

- 表示されるカラムの詳細については、侵入イベント フィールド （4 ページ）を参照してください。
- ホストのプロファイルを表示するには、ホスト IP アドレスの横に表示される [ホストプロファイル（Host Profile）] をクリックします。
- 地理位置情報の詳細を表示するには、[送信元の国（Source Country）] または [宛先の国（Destination Country）] 列に表示されるフラグをクリックします。

- システムの外部にある利用可能なソース内のデータを表示するには、イベント値を右クリックします。表示されるオプションはデータ タイプによって異なり、パブリック ソースが含まれます。他のソースは設定したリソースによって異なります。詳細については、Web ベースのリソースを使用したイベントの調査を参照してください。
- イベントに関する一般的なインテリジェンスを収集するには、テーブルでイベントの値を右クリックして、シスコまたはサードパーティのインテリジェンス ソースを選択します。たとえば、不審な IP アドレスに関する詳細情報を Cisco Talos から入手できます。表示されるオプションは、データタイプやシステムに設定されている統合によって異なります。詳細については、Web ベースのリソースを使用したイベントの調査を参照してください。
- 表示されたイベントの時刻と日付の範囲を変更するには、時間枠の変更を参照してください。

  ヒント 侵入イベントがイベント ビューに表示されない場合、指定した時間範囲を調整すると、結果が返される場合があります。古い時間範囲を指定した場合、その時間範囲内のイベントが削除されることがあります。ルールのしきい値の設定を調整すると、イベントが生成される場合があります。

  （注） イベント ビューを時間によって制約している場合は、（グローバルかイベント固有かに関係なく）アプライアンスに設定されている時間枠の外で生成されたイベントがイベント ビューに表示されます。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。

- 現在のワークフロー ページのイベントをソートする、または現在のワークフロー ページ内で移動するには、ワークフローの使用を参照してください。
- 現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフローページの左上にある該当するページ リンクをクリックします。
- イベント データベースからイベントを削除するには、削除するイベントの横にあるチェックボックスをオンにし、[削除（Delete）] または [すべて削除（Delete All）] をクリックします。
- イベントに確認済みのマークを付けて、侵入イベントのページからそれらを削除し、イベント データベースからは削除しないようにするには、侵入イベントを確認済みとしてマーク （20 ページ）を参照してください。
- 選択したイベントをトリガーしたパケットのローカル コピー（libpcap 形式のパケット キャプチャ ファイル）をダウンロードするには、ダウンロードするパケットによってトリガーされたイベントの横にあるチェックボックスをオンにして、[パケットのダウンロード（Download Packets）] または [すべてのパケットのダウンロード（Download All Packets）] をクリックします。キャプチャされたパケットは libpcap 形式で保存されます。この形式は、複数の一般的なプロトコル アナライザで使用されます。
- 他のイベント ビューに移動して関連イベントを表示するには、ワークフロー間のナビゲーションを参照してください。

- 別のワークフローを一時的に使用するには、[(ワークフローの切り替え)（(switch workflow)）] をクリックします。
- 現在のページにすぐに戻れるようにページをブックマークするには、[このページをブックマーク（Bookmark This Page）] をクリックします。
- [サマリー ダッシュボード（Summary Dashboard）] の [侵入イベント（Intrusion Events）] セクションを表示するには、[ダッシュボード（Dashboards）] をクリックします。
- ブックマークの管理ページに移動するには、[ブックマークの表示（View Bookmarks）] をクリックします。
- 現在のビューのデータに基づいてレポートを生成するには、イベント ビューからのレポート テンプレートの作成を参照してください。

関連トピック

イベントの検索
ブックマーク

侵入イベント ドリルダウン ページの制約

次の表では、ドリルダウン ページの使用方法について説明します。

表 *5:* ドリルダウン ページでのイベントの制約

目的	操作
次のワークフロー ページのドリルダウンを特定の値に制約する	値をクリックします。 たとえば、[宛先ポート（Destination Port）] ワークフローで、イベントを宛先がポート 80 であるものに制約するには、[DST ポート/ICMP コード（DST Port/ICMP Code）] 列で [80/tcp] をクリックします。ワークフローの次のページ [イベント（Events）] が表示され、ポート 80/tcp のイベントだけが含まれます。

目的	操作
次のワークフロー ページのドリルダウンを選択したイベントに制約する	次のワークフロー ページで表示するイベントの横にあるチェックボックスを選択し、[表示（View）] をクリックします。 たとえば、[宛先ポート（Destination Port）] ワークフローで、イベントを宛先がポート 20/tcp および 21/tcp であるものに制約するには、それらのポートの行の横にあるチェックボックスを選択し、[表示（View）] をクリックします。ワークフローの次のページ [イベント（Events）] が表示され、ポート 20/tcp および 21/tcp のイベントだけが含まれます。 複数の行を制約し、テーブルに複数の列が存在する場合（[数（Count）] 列を含まない）は、複合制約と呼ばれるものが作成されることに注意してください。複合制約により、必要以上のイベントを制約に含めないようにすることができます。たとえば、[イベント（Event）] と [宛先（Destination）] のワークフローを使用する場合は、最初のドリルダウン ページで選択した各行により、複合制約が作成されます。宛先 IP アドレス 10.10.10.100 のイベント 1:100 を選択し、宛先 IP アドレス 192.168.10.100 のイベント 1:200 も選択した場合、複合制約により、イベント タイプとして 1:100 を含むイベントや宛先 IP アドレスとして 192.168.10.100 を含むイベント、またはイベント タイプとして 1:200 を含むイベントや宛先 IP アドレスとして 10.10.10.100 を含むイベントが選択されないようになります。
現在の制約を保持しながら、次のワークフロー ページをドリルダウンする	[すべて表示（View All）] をクリックします。

侵入イベント テーブル ビューの制約

次の表では、テーブル ビューの使用方法について説明します。

表 *6*: イベントのテーブル ビューでのイベントの制約

目的	操作
1 つの属性を持つイベントにビューを制約する	属性をクリックします。 たとえば、宛先がポート 80 であるイベントにビューを制約するには、[DST ポート/ICMP コード（DST Port/ICMP Code）] 列で [80/tcp] をクリックします。
テーブルから列を削除する	非表示にする列の見出しで、[閉じる（Close）]（×）をクリックします。表示されるポップアップ ウィンドウで、[適用（Apply）] をクリックします。 他のカラムを表示または非表示にするには、[適用（Apply）] をクリックする前に、該当するチェックボックスをオンまたはオフにします。無効にした列をビューに戻すには、**展開の矢印** をクリックして検索の制約を展開し、[無効な列（Disabled Columns）] の下の列名をクリックします。

目的	操作
1つ以上のイベントに関連付けられたパケットを表示する	次のいずれかを行います。 • パケットを表示するイベントの横にある**下矢印** をクリックします。 • パケットを表示する1つ以上のイベントを選択し、ページの下部にある [表示（View）] をクリックします。 • ページの下部で、[すべて表示（View All）] をクリックして、現在の制約に一致するすべてのイベントのパケットを表示します。

侵入イベント パケット ビューの使用

パケット ビューは、侵入イベントを生成したルールをトリガーとして使用したパケットに関する情報を表示します。

ヒント イベントを検出するデバイスで [パケットの転送（Transfer Packet）] オプションが無効になっている場合、Secure Firewall Management Center でのパケット ビューにはパケット情報は含まれません。

パケット ビューは、パケットがトリガーとして使用した侵入イベントに関する情報を提供することによって、イベントのタイムスタンプ、メッセージ、分類、優先度、イベントを生成したルール（イベントが標準テキスト ルールによって生成された場合）など、特定のパケットがキャプチャされた理由を示します。パケット ビューは、パケットのサイズなど、パケットに関する一般情報も表示します。

さらに、パケット ビューにはパケット内の各層（データ リンク、ネットワーク、およびトランスポート）について説明したセクションと、パケットを構成するバイトについて説明したセクションがあります。システムがパケットを復号化した場合は、復号化されたバイトを表示できます。折りたたまれたセクションを展開すると、詳細情報を参照できます。

（注） それぞれのポートスキャン イベントは複数のパケットによってトリガーとして使用されるため、ポートスキャン イベントは特別なバージョンのパケット ビューを使用します。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ1 侵入イベント テーブル ビューの制約 （29 ページ）の説明に従って、侵入イベントのテーブル ビューで、表示するパケットを選択します。

ステップ 2 複数のイベントを選択した場合は、オプションで、ページの下部にあるページ番号を使用することによって、パケット ビューでパケットのページを切り替えることができます。

ステップ 3 次のオプションもあります。

- 調整：パケット ビューで日時範囲を変更するには、時間枠の変更を参照してください。
- 設定：イベントをトリガした侵入ルールを設定するには、[アクション（Actions）]の横にある矢印をクリックし、パケット ビュー内での侵入ルールの設定 （35 ページ）の説明に従って操作を続けます。
- 削除：データベースからイベントを削除するには、[削除（Delete）] をクリックして表示しているパケットのイベントを削除するか、[すべて削除（Delete All）]をクリックして以前に選択したパケットのすべてのイベントを削除します。
- ダウンロード：イベントをトリガーしたパケットのローカル コピー（libpcap 形式のパケット キャプチャ ファイル）をダウンロードするには、[パケットのダウンロード（Download Packet）]をクリックして表示しているイベントに関するキャプチャしたパケットのコピーを保存するか、[すべてのパケットをダウンロード（Download All Packets）] をクリックして以前に選択したパケットのすべてのイベントのキャプチャしたパケットのコピーを保存します。キャプチャされたパケットは libpcap 形式で保存されます。この形式は、複数の一般的なプロトコル アナライザで使用されます。

  （注） 単一のポートスキャン イベントは複数のパケットに基づいているため、ポートスキャン パケットをダウンロードできません。ただし、ポートスキャン ビューは使用可能なすべてのパケット情報を提供します。ダウンロードするには少なくとも 15 % の使用可能なディスク領域が必要です。

- 確認済みのマークを付ける：イベント データベースからは削除せずに、イベント ビューから削除するため確認済みのイベントにマークを付けるには、[確認（Review）]をクリックして表示しているパケットのイベントにマークを付けるか、[すべて確認（Review All）] をクリックして以前に選択したパケットのすべてのイベントにマーク付けます。 詳細については、侵入イベントを確認済みとしてマーク （20 ページ）を参照してください。
- 追加情報の表示：ページセクションを展開したり、折りたたんだりするには、セクションの横にある矢印をクリックします。詳細については、イベント情報のフィールド （32 ページ）、フレーム情報のフィールド （39 ページ）、データリンク層情報フィールド （40 ページ）を参照してください。
- ネットワーク層の情報の表示：ネットワーク層情報の表示 （41 ページ）を参照してください。
- パケット バイト情報の表示：パケット バイト情報の表示 （47 ページ）を参照してください。
- トランスポート層の情報の表示：次を参照してください。 トランスポート層情報の表示 （44 ページ）

関連トピック

ポートスキャン検出

イベント情報のフィールド

パケット ビューで、[イベント情報（Event Information）] セクションのパケットに関する情報を表示できます。

イベント

イベントのメッセージ。ルールベースのイベントの場合、これはルール メッセージに対応します。他のイベントの場合、これはデコーダまたはプリプロセッサによって決まります。

イベントの ID は、(GID:SID:Rev) の形式でメッセージに付加されます。GID は、ルール エンジン、デコーダ、またはイベントを生成したプリプロセッサのジェネレータ ID です。SID は、ルール、デコーダ メッセージ、またはプリプロセッサ メッセージの ID です。Rev はルールのリビジョン番号です。

Timestamp

パケットがキャプチャされた時刻（UTC タイム ゾーン）。

分類（Classification）

イベントの分類。ルールベースのイベントの場合、これはルールの分類に対応します。他のイベントの場合、これはデコーダまたはプリプロセッサによって決まります。

プライオリティ

イベントの優先度。ルールベースのイベントの場合、これは `priority` キーワードの値または `classtype` キーワードの値に対応します。他のイベントの場合、これはデコーダまたはプリプロセッサによって決まります。

入力セキュリティ ゾーン（Ingress Security Zone）

イベントをトリガーとして使用したパケットの入力セキュリティ ゾーン。パッシブ展開環境では、このセキュリティ ゾーン フィールドだけに入力されます。

出力セキュリティ ゾーン（Egress Security Zone）

イベントをトリガーとして使用したパケットの出力セキュリティ ゾーン。パッシブ展開では、このフィールドには入力されません。

ドメイン（Domain）

管理対象デバイスが属するドメイン。このフィールドは、マルチテナンシーのために Management Center を設定したことがある場合に表示されます。

デバイス

アクセス コントロール ポリシーが展開された管理対象デバイス。

セキュリティ コンテキスト（Security Context）

トラフィックが通過した仮想ファイアウォール グループを識別するメタデータ。マルチ コンテキスト モードの ASA FirePOWER の場合に、システムがこのフィールドにデータを設定することに注意してください。

入力インターフェイス（Ingress Interface）

イベントをトリガーとして使用したパケットの入力インターフェイス。パッシブ インターフェイスの場合、このインターフェイスの列だけに入力されます。

出力インターフェイス（Egress Interface）

インラインセットの場合、イベントをトリガーとして使用したパケットの出力インターフェイス。

送信元/宛先 IP（Source/Destination IP）

イベントをトリガーとして使用したパケットの発生元（送信元）であるホスト IP アドレスまたはドメイン名、またはイベントをトリガーとして使用したトラフィックのターゲット（宛先）ホスト。

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

イベントをトリガーとして使用したパケットの送信元ポート。ICMP トラフィックの場合は、ポート番号がないため、システムは ICMP タイプを表示します。

送信先ポート/ICMP コード（Destination Port/ICMP Code）

トラフィックを受信するホストのポート番号。ICMP トラフィックの場合は、ポート番号がないため、システムは ICMP コードを表示します。

電子メールのヘッダー（Email Headers）

電子メールのヘッダーから取得したデータ。電子メールのヘッダーは侵入イベントのテーブル ビューには表示されませんが、電子メール ヘッダー データは検索条件として使用できることに注意してください。

電子メールのヘッダーを SMTP トラフィックの侵入イベントと関連付けるには、SMTP プリプロセッサの [ヘッダーのログ（Log Headers）] オプションを有効にする必要があります。ルールベースのイベントの場合、この行は電子メール データが取得されたときに表示されます。

HTTP ホスト名（HTTP Hostname）

（存在する場合）HTTP 要求のホスト ヘッダーから取得されたホスト名。この行には、最大 256 バイトの完全なホスト名が表示されます。ホスト名が 1 行より長い場合は、完全なホスト名を展開できます。

ホスト名を表示するには、HTTP 検査プリプロセッサ [ホスト名のログ（Log Hostname）] オプションを有効にする必要があります。

HTTP要求パケットにホスト名が常に含まれているわけではないことに注意してください。ルールベースのイベントの場合、この行はパケットにHTTPホスト名またはHTTP URIが含まれる場合に表示されます。

HTTP URI

（存在する場合）侵入イベントをトリガーとして使用したHTTP要求パケットに関連付けられたraw URI。この行には、最大2048バイトの完全なURIが表示されます。URIが1行より長い場合は、完全なURIを展開できます。

URIを表示するには、HTTP検査プリプロセッサ[URIのログ（Log URI）]オプションを有効にする必要があります。

HTTP要求パケットにURIが常に含まれているわけではないことに注意してください。ルールベースのイベントの場合、この行はパケットにHTTPホスト名またはHTTP URIが含まれる場合に表示されます。

HTTP応答によってトリガーとして使用された侵入イベントの関連HTTP URIを参照するには、[両方のポートでのストリーム再構成の実行（Perform Stream Reassembly on Both Ports）]オプションにHTTPサーバのポートを設定する必要があります。ただし、これにより、トラフィックのリアセンブル用のリソース要求が増加することに注意してください。

侵入ポリシー（Intrusion Policy）

（存在する場合）侵入イベントを生成した侵入、プリプロセッサ、デコーダのルールが有効にされた侵入ポリシー。アクセス コントロール ポリシーのデフォルト アクションとして侵入ポリシーを選択するか、アクセス コントロール ルールと侵入ポリシーを関連付けることができます。

アクセス コントロール ポリシー（Access Control Policy）

イベントを生成した侵入ルール、プリプロセッサ ルール、またはデコーダ ルールが有効にされた侵入ポリシーが含まれるアクセス コントロール ポリシー。

アクセス コントロール ルール（Access Control Rule）

イベントを生成した侵入ルールと関連付けられたアクセス コントロール ルール。[デフォルト アクション（Default Action）]は、ルールが有効にされた侵入ポリシーがアクセス コントロール ルールに関連付けられていないことと、代わりにアクセス コントロール ポリシーのデフォルト アクションとして設定されていることを示します。

ルール（Rule）

標準テキスト ルール イベントの場合、イベントを生成したルール。

イベントが、共有オブジェクト ルール、デコーダ、またはプリプロセッサに基づいている場合は、ルールを使用できないことに注意してください。

ルールデータにはネットワークに関する機密情報が含まれるため、管理者はユーザがローカルルールの表示権限を使用してパケット ビューでルール情報を表示できる機能を、ユーザ ロール エディタで切り替えることができます。

アクション（Actions）

標準テキスト ルールとカスタム ルールのイベントの場合は、[アクション（Actions）] を展開して、イベントをトリガーとして使用したルールに次の操作のいずれかを実行します。

- ルールを編集する
- ルールのバージョンのドキュメントを表示します。標準的なテキストルールのみの場合、[アクション（Actions）] から [ドキュメントの表示（View Documentation）] をクリックした後、ドキュメントのポップアップ ウィンドウの [ルール ドキュメント（Rule Documentation）] をクリックすると、より具体的なルールの詳細を表示することができます。
- ルールにコメントを追加する
- ルールの状態を変更する
- ルールのしきい値を設定する
- ルールを抑制する

イベントが、共有オブジェクトルール、デコーダ、またはプリプロセッサに基づいている場合は、ルールを使用できないことに注意してください。

パケット ビュー内での侵入ルールの設定

侵入イベントのパケットビュー内で、イベントをトリガーとして使用したルールに対して複数のアクションを実行できます。イベントが、共有オブジェクトルール、デコーダ、またはプリプロセッサに基づいている場合は、ルールを使用できないことに注意してください。

手順

ステップ 1 侵入ルールによって生成された侵入イベントのパケット ビュー内で、[イベント情報（Event Information）] セクションの [アクション（Actions）] を展開します。

ステップ 2 次の選択肢があります。

- コメント：標準テキスト ルール イベントの場合、[ルール コメント（Rule Comment）] をクリックして、イベントを生成したルールにテキスト コメントを追加します。これにより、ルールや、特定されたエクスプロイトまたはポリシー違反に関するコンテキストおよび情報を提供できます。さらに、侵入ルールエディタでルールのコメントの追加および表示を行うこともできます。
- 無効化：このルールを無効にするには、次のオプションのいずれかをクリックします。
  - **現在のSnort 2ポリシー（<policy_name>）でこのルールを無効にします（Disable this rule in the current Snort 2 policy (<policy_name>)）**

- **ローカルで作成されたすべてのSnort 2ポリシーでこのルールを無効にします（Disable this rule in all locally created Snort 2 policies）**

このイベントが標準テキストルールによって生成された場合は、必要に応じてルールを無効にできます。ローカルで編集できるすべてのポリシーにルールを設定できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみにルールを設定することもできます。

現在のポリシーオプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタムポリシーを編集できますが、システムが提供するデフォルト ポリシーは編集できません。

（注） パケット ビューから共有オブジェクト ルールを無効にしたり、デフォルトのポリシーでルールを無効にしたりすることはできません。

- パケットのドロップとイベントの生成：トリガー元になったパケットをドロップしてイベントを生成するルールを設定するには、次のオプションのいずれかをクリックします。
  - **トリガーパケットをドロップし、現在のSnort 2ポリシー（<policy_name>）でイベントを生成するには、このルールを設定します（Set this rule to drop the triggering packet and generate an event in the current Snort 2 policy (<policy_name>)）**
  - **トリガーパケットをドロップし、ローカルで作成されたすべてのSnort 2インラインポリシーでイベントを生成するには、このルールを設定します（Set this rule to drop the triggering packet and generate an event in all locally created Snort 2 inline policies）**

管理対象デバイスがネットワーク上でインライン展開されている場合、イベントをトリガーとして使用したルールを設定して、ローカルで編集できるすべてのポリシーでルールをトリガーするパケットをドロップできます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみにルールを設定することもできます。

現在のポリシーオプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタムポリシーを編集できますが、システムが提供するデフォルト ポリシーは編集できません。このオプションは [インラインの場合ドロップ（Drop when Inline）] が現在のポリシーで有効になっている場合のみ表示されることに注意してください。

- 編集：標準テキストルールイベントの場合、[編集（Edit）]（Snort 2 を編集する場合）または [Snort 3ルールの編集（Edit Snort 3 Rule）] をクリックして、イベントを生成したルールを編集します。イベントが、共有オブジェクトルール、デコーダ、またはプリプロセッサに基づいている場合は、ルールを使用できません。

（注） システムによって提供された（カスタム標準テキストルールではない）ルールを編集する場合、実際には新規のローカルルールを作成していることになります。ローカルルールを設定して、イベントを生成し、現在の侵入ポリシーで元のルールを無効にしていることを確認してください。ただし、デフォルトのポリシーのローカルルールは有効にできないことに注意してください。

- イベントの生成：[ローカルで作成されたすべてのSnort 2ポリシーでイベントを生成するには、このルールを設定します（Set this rule to generate events in all locally created Snort 2 policies）] をクリックして、イベントを生成するルールを設定します。

  このイベントが標準テキストルールによって生成された場合は、ルールを設定して、ローカルで編集できるすべてのポリシーでイベントを生成できます。

  現在のポリシーオプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタムポリシーを編集できますが、システムが提供するデフォルト ポリシーは編集できません。

  （注） 共有オブジェクト ルールでパケット ビューからイベントを生成したり、デフォルト ポリシーでルールを無効にしたりすることはできません。

- 抑制オプションの設定：パケット ビュー内での抑制オプションの設定 （38 ページ）の説明に従って、[抑制オプションの設定（Set Suppression Options）] を展開し、続行します。

  このオプションを使用して、ローカルで編集できるすべてのポリシーで、このイベントをトリガーとして使用したルールを抑制できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみでルールを制約することもできます。

  現在のポリシーオプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタムポリシーを編集できますが、シスコが提供するデフォルト ポリシーは編集できません。

- しきい値オプションの設定：パケット ビュー内でのしきい値オプションの設定 （37 ページ）の説明に従って、[しきい値オプションの設定（Set Thresholding Options）] を展開し、続行します。

  このオプションを使用して、ローカルで編集できるすべてのポリシーでも、これをトリガーとして使用したルールのしきい値を作成できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）でのみしきい値を作成することもできます。

  現在のポリシーオプションは、現在のポリシーを編集できる場合にのみ表示されることに注意してください。たとえば、カスタムポリシーは編集できますが、システムが提供するデフォルトの侵入ポリシーは編集できません。

- ドキュメントの表示：[ドキュメントの表示（View Documentation）] をクリックして、イベントを生成したルールの説明を確認します。次に、必要に応じて [ルール ドキュメンテーション（Rule Documentation）] をクリックして、ルールの詳細を表示します。

パケット ビュー内でのしきい値オプションの設定

侵入イベントのパケットビューでしきい値オプションを設定することによって、ルールごとに時間の経過とともに生成されるイベントの数を制御できます。ローカルで編集できるすべてのポリシーに、またはローカルで編集できる場合は現在のポリシー（つまり、イベントを生成したポリシー）のみに、しきい値オプションを設定できます。

手順

ステップ 1 侵入ルールによって生成された侵入イベントのパケット ビュー内で、[イベント情報（Event Information）] セクションの [アクション（Actions）] を展開します。

ステップ 2 [しきい値オプションの設定（Set Thresholding Options）] を展開し、次の 2 つの有効なオプションから 1 つを選択します。

- 現在のSnort 2ポリシー（<policy_name>）（in the current Snort 2 policy (<policy_name>)）
- ローカルで作成されたすべてのSnort 2ポリシー（in all locally created Snort 2 policies）

ステップ 3 設定するしきい値のタイプを選択します。

- 通知を期間ごとに指定したイベント インスタンスの数に制限する場合は、[制限（limit）] をクリックします。
- 期間ごとに指定したイベント インスタンス数に達するたびに通知を行う場合は、[しきい値（threshold）] をクリックします。
- 指定されたイベント インスタンス数に達した後で、期間あたり 1 回ずつ通知を行う場合は、[両方（Both）] をクリックします。

ステップ 4 該当するしきい値をクリックして、イベントインスタンスを [送信元（Source）] IP アドレスと [宛先（Destination）] IP アドレスのどちらで追跡するかを指定します。

ステップ 5 [カウント（Count）] フィールドに、しきい値として使用するイベント インスタンスの数を入力します。

ステップ 6 [秒（Seconds）] フィールドに、イベント インスタンスを追跡する期間を指定する数（1 ～ 86400）を入力します。

ステップ 7 既存の侵入ポリシーでこのルールの現在のしきい値をオーバーライドする場合は、[このルールの既存の設定をオーバーライドする（Override any existing settings for this rule）] チェックボックスをオンにします。

ステップ 8 [しきい値の保存（Save Thresholding）] をクリックします。

パケット ビュー内での抑制オプションの設定

抑制オプションを使用して、侵入イベントをまとめて、または送信元 IP アドレスまたは宛先 IP アドレスに基づいて抑制できます。ローカルで編集できるすべてのポリシーで抑制オプションを設定できます。または、現在のポリシーをローカルで編集できる場合は、現在のポリシー（つまり、イベントを生成したポリシー）のみに抑制オプションを設定することもできます。

手順

ステップ 1 侵入ルールによって生成された侵入イベントのパケット ビュー内で、[イベント情報（Event Information）] セクションの [アクション（Actions）] を展開します。

ステップ 2 [抑制オプションの設定（Set Suppression Options）] を展開し、次の 2 つの有効なオプションから 1 つを選択します。

- 現在のSnort 2ポリシー（<policy_name>）（in the current Snort 2 policy (<policy_name>)）
- ローカルで作成されたすべてのSnort 2ポリシー（in all locally created Snort 2 policies）

（注） 現在のポリシーオプションは、現在のポリシーを編集できる場合にのみ表示されます。たとえば、カスタムポリシーを編集できますが、シスコが提供するデフォルトポリシーは編集できません。

ステップ 3 次のいずれかの [追跡対象（Track By）] オプションを選択します。

- 指定した送信元 IP アドレスから送信されるパケットによって生成されるイベントを抑制する場合は、[送信元（Source）] をクリックします。
- 指定した宛先 IP アドレスに送信されるパケットによって生成されるイベントを抑制する場合は、[宛先（Destination）] をクリックします。
- このイベントをトリガーしたルールのイベントを完全に抑制する場合は、[ルール（Rule）] をクリックします。

ステップ 4 [IP アドレス（IP address）] または [CIDR ブロック（CIDR block）] フィールドに、送信元または宛先 IP アドレスとして指定する IP アドレスまたは CIDR ブロック/プレフィクス長を入力します。

ステップ 5 [抑制の保存（Save Suppression）] をクリックします。

関連トピック

IP アドレスの規則

フレーム情報のフィールド

パケット ビューで、[フレーム（Frame）] の横にある矢印をクリックして、キャプチャされたフレームに関する情報を表示します。パケット ビューには単一フレームまたは複数フレームを表示できます。各フレームには、個々のネットワークのパケットに関する情報が表示されます。たとえば、タグ付きパケットまたは再構成された TCP ストリーム内のパケットの場合、複数のフレームが表示されます。

フレーム n（Frame n）

キャプチャされたフレーム。*n* は単一フレーム パケットの場合は 1、複数フレーム パケットの場合は差分フレーム番号です。フレーム内のキャプチャされたバイト数はフレーム番号に追加されます。

到着時間（Arrival Time）

フレームがキャプチャされた日時。

キャプチャ済みのフレームの時間デルタ（Time delta from previous captured frame）

複数フレーム パケットの場合、前のフレームがキャプチャされてからの経過時間。

表示済みのフレームの時間デルタ（Time delta from previous displayed frame）

複数フレーム パケットの場合、前のフレームが表示されてからの経過時間。

参照以降または先頭フレームからの時間（Time since reference or first frame）

複数フレーム パケットの場合、最初のフレームがキャプチャされてからの経過時間。

フレーム番号（Frame Number）

差分フレーム番号。

フレーム長（Frame Length）

フレームの長さ（バイト単位）。

キャプチャ長（Capture Length）

キャプチャされたフレームの長さ（バイト単位）。

フレームはマーク済み（Frame is marked）

フレームがマークされているかどうか（true または false）。

フレーム内のプロトコル（Protocols in frame）

フレームに含まれるプロトコル。

関連トピック

tag キーワード
TCP ストリームの再構成

データリンク層情報フィールド

パケット ビューで、データリンク層プロトコル（たとえば、[イーサネット II（Ethernet II）]）の横にある矢印をクリックして、パケットに関するデータリンク層情報を表示します。これには、送信元ホストおよび宛先ホストの 48 ビットの Media Access Control（MAC）アドレスが含まれます。ハードウェア プロトコルに応じて、パケットに関する他の情報も表示されることがあります。

（注） この例では、イーサネット リンク層情報について説明していることに注意してください。他のプロトコルも表示されることがあります。

パケット ビューはデータリンク層で使用されるプロトコルを反映します。次のリストでは、パケット ビューでイーサネット II または IEEE 802.3 イーサネット パケットについて参照できる情報について説明します。

[接続先（Destination）]

宛先ホストの MAC アドレス。

（注） イーサネットは、宛先アドレスとしてマルチキャストおよびブロードキャストアドレスを使用することもできます。

ソース（Source）

送信元ホストの MAC アドレス。

タイプ（Type）

イーサネットIIパケットの場合、イーサネットフレームでカプセル化されるパケットの種類。たとえば、IPv6 または ARP データグラム。この項目はイーサネット II パケットの場合にのみ表示されることに注意してください。

長さ（Length）

IEEE 802.3イーサネットパケットの場合、チェックサムを含まないパケットのトータル長（バイト単位）。この項目は IEEE 802.3 イーサネット パケットの場合にのみ表示されることに注意してください。

ネットワーク層情報の表示

手順

パケット ビューで、パケットにネットワーク層プロトコル（たとえば、[インターネット プロトコル（Internet Protocol）]）の横にある矢印をクリックして、パケットに関連したネットワーク層の情報の詳細情報を表示します。

（注） この例では、IPパケットについて説明していることに注意してください。他のプロトコルも表示されることがあります。

IPv4 ネットワーク層の情報フィールド

以下のリストは、IPv4パケットで表示される可能性があるプロトコル固有の情報の説明です。

バージョン（Version）

インターネット プロトコルのバージョン番号。

ヘッダー長（Header Length）

すべての IP オプションを含む、見出しのバイト数。オプションのない IP 見出しの長さは 20 バイトです。

差別化サービス フィールド（Differentiated Services Field）

送信元ホストが明示的輻輳通知（ECN）サポートする方法を示す次の差別化サービスの値。

- `0x0`：ECN-Capable Transport（ECT）をサポートしません
- `0x1` および `0x2`：ECT をサポートします
- `0x3`：Congestion Experienced（CE）

トータル長（Total Length）

IP 見出しを差し引いた IP パケットの長さ（バイト単位）。

ID

送信元ホストから送信される IP データグラムを一意的に識別する値。この値は同じデータグラム フラグメントをトレースするために使用されます。

フラグ（Flags）

IP フラグメンテーションを制御する値。

[最後のフラグメント（Last Fragment）] フラグの値は、データグラムに関連付けられた追加のフラグメントが存在するかどうかを次のように示します。

- `0`：データグラムに関連付けられた追加のフラグメントは存在しない
- `1`：データグラムに関連付けられた追加のフラグメントが存在する

[フラグメント禁止（Don’t Fragment）] フラグの値は、データグラムをフラグメント化できるかどうかを次のように制御します。

- `0`：データグラムをフラグメント化できる
- `1`：データグラムをフラグメント化**してはならない**

フラグメント オフセット（Fragment Offset）

データグラムの先頭からのフラグメント オフセットの値。

存続可能時間（ttl）（Time to Live (ttl)）

データグラムが期限切れになる前にデータグラムがルータ間で作成できるホップの数。

プロトコル

IP データグラムにカプセル化されるトランスポート プロトコル。たとえば、ICMP、IGMP、TCP、または UDP。

ヘッダー チェックサム（Header Checksum）

IP チェックサムが有効かどうかを示すインジケータ。チェックサムが無効な場合、データグラムが送信中に破損したか、侵入回避の試行において使用中である可能性があります。

送信元または送信先（Source/Destination）

送信元（または宛先）ホストの IP アドレスまたはドメイン名。

ドメイン名を表示するには、IP アドレス解決を有効にする必要があることに注意してください。

アドレスまたはドメイン名をクリックしてコンテキストメニューを表示してから、whois 検索を実行する場合は [Whois] を、ホスト情報を表示する場合は [ホストプロファイルの表示（View Host Profile）] を、アドレスをグローバルブロックリストまたはブロックしないリストに追加するオプションを選択します。

IPv6 ネットワーク層の情報フィールド

以下のリストは、IPv6 パケットで表示される可能性があるプロトコル固有の情報の説明です。

トラフィック クラス（Traffic Class）

IPv4 で提供される差別化サービス機能と同じように、IPv6 パケット クラスまたは優先度を特定する IPv6 見出し内の Experimental 8 ビットのフィールド。未使用の場合、このフィールドはゼロに設定されます。

フロー ラベル（Flow Label）

非デフォルトの QoS またはリアルタイム サービスなどの特別なフローを特定する、1 から FFFF までの、オプションの 20 ビットの IPv6 16 進数値。未使用の場合、このフィールドはゼロに設定されます。

ペイロード長（Payload Length）

IPv6 ペイロードのオクテットの数を特定する 16 ビット フィールド。これは、任意の拡張子見出しを含む、IPv6 見出しに続くすべてのパケットで構成されます。

次ヘッダー（Next Header）

IPv4 プロトコル フィールドと同じ値を使用して、IPv6 見出しのすぐ後に続く、見出しの種類を特定する 8 ビットのフィールド。

ホップ リミット（Hop Limit）

パケットを転送するノードごとに 1 つずつデクリメントする 8 ビットの 10 進整数。デクリメントした値がゼロになると、パケットは破棄されます。

ソース（Source）

送信元ホストの 128 ビットの IPv6 アドレス。

[接続先（Destination）]

宛先ホストの 128 ビットの IPv6 アドレス。

トランスポート層情報の表示

手順

ステップ 1 パケット ビューで、トランスポート層プロトコル（たとえば [TCP]、[UDP]、または [ICMP]）の横にある矢印をクリックします。

ステップ 2 オプションで、存在する場合、[データ（Data）] をクリックして、パケット ビューの [パケット情報（Packet Information）] セクションで、プロトコルのすぐ上にあるペイロードの最初の 24 バイトを表示します。

ステップ 3 TCP パケット ビューのフィールド （44 ページ）、UDP パケット ビューのフィールド （45 ページ）、またはICMP パケット ビュー フィールド （46 ページ）の説明に従って、TCP、UDP、ICMP プロトコルのトランスポート層の内容を表示します。

（注） これらの例では、TCP、UDP、ICMP パケットについて説明していますが、他のプロトコルも表示されることがあることに注意してください。

TCP パケット ビューのフィールド

ここでは、TCP パケットのプロトコル固有の情報について説明します。

ソース ポート

発信元のアプリケーション プロトコルを識別する番号。

接続先ポート（Destination port）

受信側のアプリケーション プロトコルを識別する番号。

シーケンス番号（Sequence number）

TCP ストリームの初期シーケンス番号と連動する、現在の TCP セグメントの最初のバイトの値。

次のシーケンス番号（Next sequence number）

応答パケットにおける、送信する次のパケットのシーケンス番号。

確認応答番号（Acknowledgement number）

以前に受信されたデータのシーケンス番号に連動した TCP 確認応答。

ヘッダー長（Header Length）

ヘッダーのバイト数。

フラグ（Flags）

TCP セグメントの転送状態を示す 6 ビット。

- `U`：緊急ポインタが有効
- `A`：確認応答番号が有効
- `P`：受信者はデータをプッシュする必要がある
- `R`：接続をリセットする
- `S`：シーケンス番号を同期して新しい接続を開始する
- `F`：送信者はデータ送信を終了した

ウィンドウ サイズ（Window size）

受信ホストが受け入れる、確認応答されていないデータの量（バイト単位）。

チェックサム（Checksum）

TCP チェックサムが有効かどうかを示すインジケータ。チェックサムが無効な場合、データグラムが送信中に破損したか、回避の試行において使用中である可能性があります。

緊急ポインタ（Urgent Pointer）

緊急データが終了する TCP セグメントの位置（存在する場合）。`U` フラグとともに使用します。

オプション（Options）

TCP オプションの値（存在する場合）。

UDP パケット ビューのフィールド

ここでは、UDP パケットのプロトコル固有の情報について説明します。

ソース ポート

発信元のアプリケーション プロトコルを識別する番号。

接続先ポート（Destination port）

受信側のアプリケーション プロトコルを識別する番号。

長さ（Length）

UDP 見出しとデータを組み合わせた長さ。

チェックサム（Checksum）

UDPチェックサムが有効かどうかを示すインジケータ。チェックサムが無効な場合、データグラムが送信中に破損した可能性があります。

ICMP パケット ビュー フィールド

ここでは、ICMP パケットのプロトコル固有の情報について説明します。

タイプ

ICMP メッセージのタイプ。

- 0：エコー応答
- 3：宛先到達不能
- 4：ソース クエンチ（始点抑制要求）
- 5：リダイレクト
- 8：エコー要求
- 9：ルータ アドバタイズメント
- 10：ルータ送信要求
- 11：時間超過
- 12：パラメータの問題
- 13：タイムスタンプ要求
- 14：タイムスタンプ応答
- 15：情報要求（廃止）
- 16：情報応答（廃止）
- 17：アドレス マスク要求
- 18：アドレス マスク応答

コード

ICMP メッセージ タイプに付随するコード。ICMP メッセージ タイプ 3、5、11、および 12 には、RFC 792 で説明されている対応コードがあります。

チェックサム（Checksum）

ICMP チェックサムが有効かどうかを示すインジケータ。チェックサムが無効な場合、データグラムが送信中に破損した可能性があります。

パケット バイト情報の表示

手順

パケット ビューで、[パケット バイト（Packet Bytes）] の横にある矢印をクリックして、パケットを構成するバイトの 16 進数および ASCII バージョンを表示します。システムがトラフィックを復号化した場合は、復号化されたパケット バイトを表示できます。

内部ソースからの侵入イベント

内部ソースからの侵入イベントは、ネットワーク上の侵害を受けたホストを示しています。ソース IP アドレスがネットワーク上にある場合は、そのホストを調査する必要があることを示しています。

侵入イベントの統計情報の表示

[侵入イベントの統計情報（Intrusion Event Statistics）] ページは、アプライアンスの現在の状態の概要と、ネットワークで生成されたすべての侵入イベントを表示します。

このページに表示される IP アドレス、ポート、プロトコル、イベント メッセージなどはそれぞれリンクになっています。関連イベントの情報を表示するには、任意のリンクをクリックします。たとえば、上位 10 個の宛先ポートのいずれかが `80 (http) /tcp` である場合、そのリンクをクリックすると、デフォルトの侵入イベント ワークフローの最初のページが表示され、そのポートをターゲットとするイベントがリストされます。現在の時刻範囲で表示されるのはイベント（およびイベントを生成する管理対象デバイス）のみであることに注意してください。さらに、確認済みマークを付けた侵入イベントも統計に引き続き表示されます。たとえば、現在の時刻範囲が過去 1 時間であり、最初のイベントが 5 時間前に生成された場合、[最初のイベント（First Event）] リンクをクリックすると、そのイベントは時刻範囲を変更するまでイベント ページには表示されません。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[概要（Overview）] > [概要（Summary）] > [侵入イベント統計（Intrusion Event Statistics）]** を選択します。

ステップ 2 ページの上部にある2つの選択ボックスから、統計を表示するゾーンおよびデバイスを選択するか、[すべてのセキュリティ ゾーン（All Security Zones）] および [すべてのデバイス（All Devices）] を選択して、侵入イベントを収集するすべてのデバイスの統計を表示します。

ステップ 3 [統計の取得（Get Statistics）] をクリックします。

ヒント カスタム時刻範囲からデータを表示するには、右上のページエリアのリンクをクリックし、時間枠の変更にある指示に従います。

ホスト統計情報

[侵入イベント統計情報（Intrusion Event Statistics）] ページの [ホスト統計情報（Host Statistics）] セクションは、アプライアンス自体に関する情報を提供します。Secure Firewall Management Center では、このセクションはすべての管理対象デバイスに関する情報も提供します。

この情報には、次の内容が含まれます。

時刻（Time）

アプライアンスの現在の時刻。

アップタイム（Uptime）

アプライアンス自体が再起動してから経過した日数、時間、および分数。Secure Firewall Management Center では、[アップタイム（Uptime）] に各管理対象デバイスの最終起動時刻、ログインしたユーザの数、および負荷平均も示されます。

ディスク使用率（Disk Usage）

使用中のディスクの割合。

メモリ使用率（Memory Usage）

使用中のシステム メモリの割合。

負荷平均（Load Average）

直前の 1 分間、5 分間、15 分間の CPU キュー内の平均プロセス数。

イベントの概要

[侵入イベント統計（Intrusion Event Statistics）] ページの [イベントの概要（Event Overview）] セクションは、侵入イベント データベースにある情報の概要を示します。

これらの統計には、次の情報が含まれています。

イベント

侵入イベント データベースのイベントの数。

時間範囲内のイベント（Events in Time Range）

現在選択されている時間範囲と、時間範囲内に収まるデータベースのイベントの割合。

最初のイベント（First Event）

イベント データベース内の最初のイベントのイベント メッセージ。

最後のイベント（Last Event）

イベント データベース内の最後のイベントのイベント メッセージ。

（注） Secure Firewall Management Center で侵入イベント データを表示中に管理対象デバイスを選択した場合は、そのデバイスの [イベントの概要（Event Overview）] セクションが代わりに表示されます。

イベント統計

[侵入イベント統計（Intrusion Event Statistics）] ページの [イベント統計（Event Statistics）] セクションでは、侵入イベント データベース内の情報に関する具体的な情報が表示されます。

この情報には、次に関する詳細が含まれます。

- 上位 10 個のイベント タイプ
- 上位 10 個の送信元 IP アドレス
- 上位 10 個の宛先 IP アドレス
- 上位 10 個の宛先ポート
- イベント数が最大であるプロトコル、イングレスとイーグレスのセキュリティ ゾーン、およびデバイス

（注） マルチドメイン展開では、システムは、各リーフ ドメインに個別のネットワーク マップを作成します。その結果、リーフ ドメインには、ネットワーク内で一意である IP アドレスを含めることができますが、別のリーフ ドメイン内の IP アドレスと同じにすることができます。先祖ドメインでイベントの統計情報を表示すると、システムで、その IP アドレスの複数のインスタンスが繰り返し表示される場合があります。一見すると、エントリが重複しているように見えることがあります。ただし、各 IP アドレスのホスト プロファイル情報までドリル ダウンすると、それらが異なるリーフ ドメインに属していることがわかります。

侵入イベントのパフォーマンス グラフの表示

[侵入イベントのパフォーマンス（Intrusion Event Performance）] ページでは、Secure Firewall Management Center または管理対象デバイスの指定された期間の侵入イベントのパフォーマンス統計情報を示すグラフを生成できます。グラフを生成することにより、1 秒あたりの侵入イベントの数、1 秒あたりのメガビット数、1 パケットあたりの平均バイト数、Snort によって検査されていないパケットの割合、および TCP 正規化の結果としてブロックされたパケットの数を反映できます。これらのグラフは、過去 1 時間、前日、先週、または先月の操作の統計を表示できます。

（注） 新しいデータは 5 分ごとに統計グラフに蓄積されます。したがって、グラフをすばやくリロードしても、次の 5 分の差分更新が実行されるまでデータは変更されていない場合があります。各グラフには、選択した時間間隔（前月、週、日、または時間）に対応した間隔（日、時間、または 5 分）で平均値が表示されます。平均値が 1 未満の場合は、小数値で表示されます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[概要（Overview）] > [概要（Summary）] > [侵入イベントパフォーマンス（Intrusion Event Performance）]**を選択します。

ステップ 2 [デバイスの選択（Select Device）] リストから、データを表示するデバイスを選択します。

ステップ 3 侵入イベントのパフォーマンス統計情報グラフの種類（50 ページ）で説明されているように、[グラフの選択（Select Graph(s)）] リストから、作成するグラフの種類を選択します。

ステップ 4 [時間範囲の選択（Select Time Range）] リストから、グラフに使用する時間範囲を選択します。

ステップ 5 [グラフ（Graph）] をクリックします。

ステップ 6 グラフを保存するには、グラフを右クリックし、ブラウザでイメージを保存する手順に従います。

侵入イベントのパフォーマンス統計情報グラフの種類

次の表に、表示可能なグラフの種類を示します。ネットワーク分析ポリシーの [インライン モード（Inline Mode）] 設定の影響を受けるデータを含むグラフ タイプでは、表示が異なるので注意してください。[インライン モード（Inline Mode）] が無効になっている場合、Web インターフェイスでアスタリスク（*）が付いているグラフタイプ（下記の表では列に [はい（yes）] と記載）には、[インライン モード（Inline Mode）] が有効になっている場合に変更またはドロップされるトラフィックに関するデータが含まれています。

表 7:侵入イベントのパフォーマンス グラフの種類

データの生成対象となるグラフ	実行する操作	説明	インラインモードによる影響
平均バイト/パケット（Avg Bytes/Packet）	適用対象外	各パケットに含まれる平均バイト数。	いいえ
TCP トラフィックまたはパケットで正規化された ECN フラグ（ECN Flags Normalized in TCP Traffic/Packet）	[明示的輻輳通知（Explicit Congestion Notification）] を有効にして、[パケット（Packet）] を選択します。	ネゴシエーションに関係なく、パケット単位で ECN フラグがクリアされたパケットの数。	Yes
TCP トラフィックまたはセッションで正規化された ECN フラグ（ECN Flags Normalized in TCP Traffic/Session）	[明示的輻輳通知（Explicit Congestion Notification）] を有効にして、[ストリーム（Stream）] を選択します。	ECN の使用がネゴシエートされなかった場合にストリーム単位で ECN フラグがクリアされた回数。	Yes
イベント/秒（Events/Sec）	適用対象外	デバイスで生成された 1 秒あたりのイベント数。	いいえ
ICMPv4 エコーの正規化（ICMPv4 Echo Normalizations）	[ICMPv4 の正規化（Normalize ICMPv4）] を有効にします。	エコー（要求）またはエコー応答メッセージの 8 ビット コード フィールドがクリアされた ICMPv4 パケットの数。	Yes
ICMPv6 エコーの正規化（ICMPv6 Echo Normalizations）	[ICMPv6 の正規化（Normalize ICMPv6）] を有効にします。	エコー（要求）またはエコー応答メッセージの 8 ビット コード フィールドがクリアされた ICMPv6 パケットの数。	Yes
IPv4 DF フラグの正規化	[IPv4 の正規化（Normalize IPv4）] と [DF ビットの正規化（Normalize Don't Fragment Bit）] を有効にします。	[IPv4 フラグ（IPv4 Flags）] ヘッダー フィールドのシングル ビット [フラグメント禁止（Don't Fragment）] サブフィールドがクリアされた IPv4 パケットの数。	Yes
IPv4 オプションの正規化（IPv4 Options Normalizations）	[IPv4 の正規化（Normalize IPv4）] を有効にします。	オプション オクテットが「1」（操作なし（No Operation））に設定された IPv4 パケットの数。	はい
IPv4 予約済みフラグの正規化	[IPv4 の正規化（Normalize IPv4）] と [予約済みビットの正規化（Normalize Reserved Bit）] を有効にします。	[IPv4 フラグ（IPv4 Flags）] ヘッダー フィールドのシングル ビット [予約済み（Reserved）] サブフィールドがクリアされた IPv4 パケットの数。	Yes

データの生成対象となるグラフ	実行する操作	説明	インラインモードによる影響
IPv4 サイズ変更の正規化（IPv4 Resize Normalizations）	[IPv4 の正規化（Normalize IPv4）] を有効にします。	超過ペイロードが IP ヘッダーで指定されたデータグラム長に切り詰められた IPv4 パケットの数。	Yes
IPv4 TOS の正規化	[IPv4 の正規化（Normalize IPv4）] と [TOS ビットの正規化（Normalize TOS Bit）] を有効にします。	1 バイトの [差別化サービス（DS）（Differentiated Services (DS)）] フィールド（旧 [タイプ オブ サービス（ToS）（Type of Service (TOS)）] フィールド）がクリアされた IPv4 パケットの数。	Yes
IPv4 TTL の正規化（IPv4 TTL Normalizations）	[IPv4 の正規化（Normalize IPv4）]、[最大 TTL（Maximum TTL）]、および [TTL のリセット（Reset TTL）] を有効にします。	IPv4 存続時間（TTL）正規化の数。	はい
IPv6 オプションの正規化（IPv6 Options Normalizations）	[IPv6 の正規化（Normalize IPv6）] を有効にします。	[ホップバイホップ オプション（Hop-by-Hop Options）] または [宛先オプション（Destination Options）] 拡張ヘッダーの [オプション タイプ（Option Type）] フィールドが、00（スキップして処理を続行）に設定された IPv6 パケットの数。	Yes
IPv6 TTL の正規化（IPv6 TTL Normalizations）	[IPv6 の正規化（Normalize IPv6）]、[最小 TTL（Minimum TTL）]、および [TTL のリセット（Reset TTL）] を有効にします。	IPv6 ホップ リミット（TTL）正規化の数。	はい
メガビット/秒（Mbits/Sec）	適用対象外	デバイスをパススルーするトラフィックの 1 秒あたりのメガビット数。	いいえ
MSS に合わせてサイズ変更されたパケットの正規化（Packet Resized to Fit MSS Normalizations）	[データを MSS にトリミング（Trim Data to MSS）] を有効にします。	ペイロードが TCP データ フィールドよりも長かったため、ペイロードが最大セグメント サイズに切り詰められたパケットの数。	はい
TCP ウィンドウに合わせてサイズ変更されたパケットの正規化（Packet Resized to Fit TCP Window Normalizations）	[データをウィンドウにトリミング（Trim Data to Window）] を有効にします。	受信側ホストの TCP ウィンドウに合わせて TCP データ フィールドが切り詰められたパケットの数。	はい

データの生成対象となるグラフ	実行する操作	説明	インラインモードによる影響
ドロップされたパケットの割合（Percent Packets Dropped）	適用対象外	選択されたすべてのデバイスにおける未検査のパケットの平均割合。たとえば、2 つのデバイスを選択した場合、平均が 50 % であるというのは、1 つのデバイスのドロップ率が 90 % であり、もう 1 つのデバイスのドロップ率が 10 % であることを示している可能性があります。また、両方のデバイスのドロップ率が 50% である可能性もあります。グラフは、1 つのデバイスを選択した場合にのみ合計ドロップ率を表します。	いいえ
データが除去された RST パケットの正規化（RST Packets With Data Stripped Normalizations）	[RST に関するデータを削除（Remove Data on RST）] を有効にします。	TCP リセット（RST）パケットからデータが削除されたパケットの数。	はい
データが除去された SYN パケットの正規化（SYN Packets With Data Stripped Normalizations）	[SYN に関するデータを削除（Remove Data on SYN）] を有効にします。	TCP オペレーティング システムが Mac OS でない場合に、SYN パケットからデータが削除されたパケットの数。	はい
TCP ヘッダー パディングの正規化（TCP Header Padding Normalizations）	[オプション パディング バイトの正規化またはクリア（Normalize/Clear Option Padding Bytes）] を有効にします。	オプションの埋め込みバイトが 0 に設定された TCP パケットの数。	はい
TCP オプションなしの正規化（TCP No Option Normalizations）	[これらの TCP オプションを許可（Allow These TCP Options）] を有効にして、[任意（any）] 以外のオプションに設定します。	タイムスタンプ オプションがストリップされたパケットの数。	はい
TCP NS フラグの正規化（TCP NS Flag Normalizations）	[明示的輻輳通知（Explicit Congestion Notification）] を有効にして、[パケット（Packet）] を選択します。	ECN Nonce Sum（NS）オプション正規化の数。	はい

データの生成対象となるグラフ	実行する操作	説明	インラインモードによる影響
TCP オプションの正規化（TCP Options Normalizations）	[これらの TCP オプションを許可（Allow These TCP Options）] を有効にして、[任意（any）] 以外のオプションに設定します。	オプション フィールドが [操作なし（No Operation）]（TCP オプション 1）に設定されているオプションの数（[MSS]、[ウィンドウ スケール（Window Scale）]、[タイム スタンプ（Time Stamp）]、および明示的に許可されたオプションを除く）。	はい
正規化によってブロックされた TCP パケット（TCP Packets Blocked By Normalizations）	[TCP ペイロードの正規化（Normalize TCP Payload）] を有効にします（セグメントのリアセンブリは失敗します）。	TCP セグメントを正常にリアセンブルできなかったためにドロップされたパケットの数。	はい
TCP 予約済みフラグの正規化（TCP Reserved Flags Normalizations）	[予約済みビットの正規化またはクリア（Normalize/Clear Reserved Bits）] を有効にします。	予約済みビットがクリアされた TCP パケットの数。	はい
TCP セグメント リアセンブリの正規化（TCP Segment Reassembly Normalizations）	[TCP ペイロードの正規化（Normalize TCP Payload）] を有効にします（セグメントのリアセンブリは成功します）。	再送信データの一貫性を確保するために [TCP データ（TCP Data）] フィールドが正規化されたパケットの数。（正しくリアセンブルできないセグメントはすべてドロップされます）。	はい
TCP SYN オプションの正規化（TCP SYN Option Normalizations）	[これらの TCP オプションを許可（Allow These TCP Options）] を有効にして、[任意（any）] 以外のオプションに設定します。	SYN 制御ビットが設定されていないため、[最大セグメント サイズ（Maximum Segment Size）] または [ウィンドウ スケール（Window Scale）] オプションが [操作なし（No Operation）]（TCP オプション 1）に設定されたオプションの数。	はい
TCP タイムスタンプ ECR の正規化（TCP Timestamp ECR Normalizations）	[これらの TCP オプションを許可（Allow These TCP Options）] を有効にして、[任意（any）] 以外のオプションに設定します。	確認応答（ACK）制御ビットが設定されていないため、[タイム スタンプ エコー応答（TSecr）（Time Stamp Echo Reply (TSecr)）] オプション フィールドがクリアされたパケットの数。	はい
TCP 緊急ポインタの正規化（TCP Urgent Pointer Normalizations）	[緊急ポインタの正規化（Normalize Urgent Pointer）] を有効にします。	TCP ヘッダーの [緊急ポインタ（Urgent Pointer）] フィールド（2 バイト）がペイロード長を超えていたため、ペイロード長に合わせて設定されたパケットの数。	Yes

データの生成対象となるグラフ	実行する操作	説明	インラインモードによる影響
ブロックされたパケットの総数（Total Blocked Packets）	[インライン モード（Inline Mode）] または [インライン時にドロップ（Drop when Inline）] を設定します。	ルール、デコーダ、およびプリプロセッサのドロップを含めて、ドロップされたパケットの総数。	いいえ
インジェクションされたパケットの総数（Total Injected Packets）	[インライン モード（Inline Mode）] を設定します。	再送信前にサイズ変更されたパケットの数。	いいえ
TCP フィルタ適用パケットの総数（Total TCP Filtered Packets）	TCP ストリームの前処理を設定します。	TCP ポートフィルタリングのためにストリームによってスキップされたパケットの数。	いいえ
UDP フィルタ適用パケットの総数（Total UDP Filtered Packets）	UDP ストリームの前処理を設定します。	UDP ポートフィルタリングのためにストリームによってスキップされたパケットの数。	いいえ
緊急フラグ クリア済みの正規化（Urgent Flag Cleared Normalizations）	[緊急ポインタが設定されていない場合 URG をクリア（Clear URG if Urgent Pointer is Not Set）] を有効にします。	緊急ポインタが設定されていなかったため、TCP ヘッダーの URG 制御ビットがクリアされたパケットの数。	はい
緊急ポインタおよび緊急フラグ クリア済みの正規化（Urgent Pointer and Urgent Flag Cleared Normalizations）	[空のペイロードに設定された緊急ポインタまたは URG をクリア（Clear Urgent Pointer/URG on Empty Payload）] を有効にします。	ペイロードがなかったため、TCP ヘッダーの [緊急ポインタ（Urgent Pointer）] フィールドと URG 制御ビットがクリアされたパケットの数。	はい
緊急ポインタ クリア済みの正規化（Urgent Pointer Cleared Normalizations）	[URG=0 の場合に緊急ポインタをクリア（Clear Urgent Pointer if URG=0）] を有効にします。	緊急（URG）制御ビットが設定されていなかったため、TCP ヘッダーの [緊急ポインタ（Urgent Pointer）] フィールド（16 ビット）がクリアされたパケットの数。	はい

関連トピック

インライン正規化プリプロセッサ
インライン導入でのプリプロセッサによるトラフィックの変更
インライン展開でのドロップ動作

侵入イベント グラフの表示

システムは、経時的な侵入イベントの傾向を示すグラフを表示します。1 つまたはすべての管理対象デバイスについて、過去1時間から先月までの範囲の経時的な侵入イベント グラフを生成できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[概要（Overview）]** > **[概要（Summary）]** > **[侵入イベントグラフ（Intrusion Event Graphs）]** を選択します。

ステップ 2 [デバイスの選択（Select Device）] で、[すべて（all）] を選択してすべてのデバイスを含めるか、グラフに含める特定のデバイスを選択します。

ステップ 3 [グラフの選択（Select Graph(s)）] で、生成するグラフの種類を選択します。

- 上位 10 個の宛先ポート
- 上位 10 個の送信元 IP アドレス
- 上位 10 個のイベント メッセージ

ステップ 4 [時間範囲の選択（Select Time Range）] で、グラフの時間範囲を選択します。

- 直近の 1 時間（Last Hour）
- 前日（Last Day）
- 先週（Last Week）
- 先月（Last Month）

ステップ 5 [グラフ（Graph）] をクリックします。

侵入イベントの履歴

機能	最小 Management Center	最小 Threat Defense	詳細
IPS イベントデータストアの交換	7.1	任意（Any）	• 侵入インシデント、侵入イベントクリップボード、およびデフォルトのカスタムテーブル（侵入イベント列（[送信元重要度を持つ侵入イベント（Intrusion Events with Source Criticality）] および [宛先重要度を持つ侵入イベント（Intrusion Events with Destination Criticality）]）を使用するテーブルは廃止されています。 [コピー（Copy）] ボタンと [すべてコピー（Copy All）] ボタンを使用してクリップボードにイベントを追加できなくなりました。 廃止されたページ： • [分析（Analysis）] > [侵入（Intrusions）] > [クリップボード（Clipboard）] • [分析（Analysis）] > [侵入（Intrusions）] > [インシデント（Incidents）] • メインの侵入イベントテーブルに、[送信元ホストの重要度（Source Host Criticality）] と [宛先ホストの重要度（Destination Host Criticality）] という新しい 2 つのフィールドが追加されました。 サポートされているプラットフォーム： Secure Firewall Management Center
Syslog の接続イベントの固有識別子	6.4.0.4	任意（Any）	syslog の [DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、接続イベントを一意に識別できます。これらのフィールドは、侵入イベントの syslog に含まれます。
[IntrusionPolicy] フィールドが syslog に含まれるようになりました。	6.4	任意（Any）	侵入イベントの syslog が、イベントをトリガーした侵入ポリシーを指定するようになりました。
新しい侵入イベント検索フィールド：[CVE ID]	6.4	任意（Any）	MITRE の Common Vulnerabilities and Exposures 番号で検索できるようになりました。 変更された画面：[分析（Analysis）] > [侵入（Intrusions）] > [イベント（Events）] > [検索の編集（Edit Search）] サポート対象プラットフォーム：すべて

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。