接続ロギング

次のトピックでは、モニター対象ネットワークでホストから実行される接続を記録するよう Firepower システムを設定する方法について説明します。

接続ロギングについて

システムは管理対象デバイスで検出された接続のログを生成できます。このログは接続イベントと呼ばれます。ルールやポリシーの設定を行うことで、ログに記録する接続の種類、接続をログに記録するタイミング、およびデータを保存する場所をきめ細かく制御できます。セキュリティ関連の接続イベントと呼ばれる特別な接続イベントは、レピュテーションベースのセキュリティ インテリジェンス機能によってブロックされた接続を表します。

接続イベントには、検出されたセッションに関するデータも含まれています。個々の接続イベントで入手可能な情報はいくつかの要因に応じて異なりますが、一般的には次のものがあります。

- タイムスタンプ、送信元と宛先の IP アドレス、入出力ゾーン、接続を処理したデバイスなど、基本的な接続特性
- アプリケーション、要求されるURL、または接続に関連付けられているユーザなど、システムによって検出または推測される追加の接続特性
- どの設定がトラフィックを処理したか、接続が許可またはブロックされていたかどうか、暗号化された接続および復号された接続に関する詳細など、接続がログに記録された理由に関するメタデータ

部門のセキュリティ上およびコンプライアンス上の要件に従って接続をロギングしてください。接続ロギングを設定する際は、システムはさまざまな理由で接続をロギングすることがあり、1 ヵ所でロギングを無効にしても一致する接続がログに記録されなくなるとは限りません。

接続イベント内の情報は、トラフィックの特性、最終的に接続を処理した設定など、いくつかの要因によって異なります。

（注） エクスポートしたNetFlowレコードから生成された接続データを使い、管理対象デバイスで収集された接続ログを補うことができます。これは、管理対象デバイスでモニターできないネットワーク上にNetFlow対応ルータやその他のデバイスを配置した場合に特に有効です。

常にログに記録される接続

接続イベントのストレージを無効にしない限り、システムは他のロギング設定に関係なく、Firewall Management Centerデータベースに次の接続終了イベントを保存します。

侵入に関連付けられた接続

システムは、接続がアクセス コントロール ポリシーのデフォルトのアクションで処理される限り、侵入イベントに関連付けられている接続を自動的に記録します。

アクセス コントロールのデフォルト アクションに関連付けられた侵入ポリシーによって侵入イベントが生成された場合、システムは、そのイベントに関連する接続の終了を自動的にログに記録しません。代わりに、デフォルトのアクション接続のロギングを明示的に有効にする必要があります。これは、接続データをログに記録する必要がない、侵入防御専用の展開環境で役立ちます。

ただし、デフォルトアクションで接続開始ロギングを有効にした場合、接続開始のロギングに加えて、関連する侵入ポリシーがトリガーしたときにシステムによって接続終了がログに記録されます。

ファイル イベントとマルウェア イベントに関連付けられた接続

システムは、ファイル イベントとマルウェア イベントに関連付けられた接続を自動的にログに記録します。

（注） NetBIOS-SSN（SMB）トラフィックのインスペクションによって生成されるファイルイベントは、即座には接続イベントを生成しません。これは、クライアントとサーバーが持続的接続を確立するためです。システムはクライアントまたはサーバーがセッションを終了した後に接続イベントを生成します。

インテリジェント アプリケーション バイパスに関連付けられた接続

システムは、IABに関連付けられたバイパスされた、およびバイパスされるはずだった接続をログに記録します。

モニタ対象の接続

システムは常に、モニタの対象のトラフィックの接続終了をロギングします。このことは、トラフィックに一致する他のルールがなく、デフォルトアクションのロギングを有効にしていない場合でも該当します。詳細については、「モニターされた監視接続のロギング （4 ページ）」を参照してください。

ログ可能なその他の接続

重要な接続のみがロギングされるように、ルールごとの接続ロギングを有効にします。あるルールに対し接続ロギングを有効にすると、システムはそのルールによって処理されたすべての接続をロギングします。

また、ポリシーのデフォルト アクションにより処理された接続をロギングすることもできます。ルールやデフォルトアクションにより（アクセス制御の場合は、ルールのインスペクション設定により）、ロギングのオプションは異なります。

プレフィルタ ポリシー：ルールとデフォルト アクション

プレフィルタ ポリシーによりファースト パスまたはブロックする接続（すべてのプレーン テキスト、パススルー トンネルを含む）をロギングすることができます。

プレフィルタは、外部ヘッダーを基準にしてトラフィックを処理します。ロギングするトンネルでは、結果の接続イベントには、外部のカプセル化ヘッダー情報が含まれます。

継続分析の対象となるトラフィックについては、一致する接続が他の設定によってロギングされることがあるかもしれませんが、プレフィルタ ポリシーによるロギングは無効となります。システムは内部ヘッダーを使ってすべての継続分析を行います。つまり、システムは、許可されたトンネル内の各接続を個別に処理、ロギングします。

復号ポリシー：ルールとデフォルトアクション

復号ルールまたは復号ポリシーのデフォルトアクションに一致する接続をロギングすることができます。

ブロックされた接続の場合、システムは即座にセッションを終了し、イベントを生成します。モニタ対象の接続とアクセス制御ルールに渡す接続では、セッションが終了する際にイベントが生成されます。

アクセス コントロール ポリシー：セキュリティ インテリジェンスによる判断

接続がレピュテーションベースのセキュリティインテリジェンス機能によってブロックされる場合は、その接続をログに記録できます。

オプションで、セキュリティ インテリジェンス フィルタリングにはモニター専用設定を使用できます。パッシブ展開環境では、この設定が推奨されます。この設定では、セキュリティインテリジェンスによってブロックされるはずの接続をシステムがさらに分析できるだけでなく、一致する接続をログに記録することもできます。セキュリティ インテリジェンス モニタリングによって、セキュリティ インテリジェンス情報を使用してトラフィック プロファイルを作成することもできます。

セキュリティ インテリジェンスのフィルタリングの結果、システムが接続イベントをロギングすると、一致するセキュリティ インテリジェンス イベントもロギングされます。そのイベントは特殊なタイプの接続イベントで、個別に表示および分析することができ、また個別に保存、プルーニングされます。一致する IP アドレスが接続にあるかどうかを識別できるように、[分析（Analysis）] > [接続（Connections）] メニューのページの表では、ブロックされ、モニターされている IP アドレスの横のホストアイコンは見た目が少し異なります。

アクセス コントロール ポリシー：ルールとデフォルト アクション

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 アクションに一致する接続をロギングすることができます。

関連トピック

ルールとポリシーのアクションによるロギングへの影響 （4 ページ）

ルールとポリシーのアクションによるロギングへの影響

接続イベントには、接続がロギングされた理由を記述したメタデータが含まれています。メタデータにはトラフィックがどの設定によって処理されたかなどの情報が含まれます。接続ロギングを設定する場合、ルール アクションおよびポリシーのデフォルト アクションにより、一致するトラフィックをシステムがどのように検査、処理するのかだけでなく、一致するトラフィックの詳細をいつ、どのようにロギングするかが決まります。

関連トピック

接続およびセキュリティ関連の接続イベントフィールド

FastPath された接続のロギング

FastPath された接続や非暗号化トンネルをロギングできます。ロギングには、プレフィルタ ポリシーの以下のルールとアクションに一致するトラフィックを含めることができます。

- トンネル ルール：[ファストパス（FastPath）] アクション（外部セッションをロギングします）
- プレフィルタ ルール：[ファストパス（FastPath）] アクション

FastPath されたトラフィックはアクセス コントロールと QoS の残りをバイパスするため、FastPath された接続の接続イベントに含まれる情報は限られます。

モニターされた監視接続のロギング

システムは常に、以下の設定と一致するトラフィックの接続終了をロギングします。このことは、トラフィックに一致する他のルールがなく、デフォルトアクションのロギングを有効にしていない場合でも該当します。

- セキュリティ インテリジェンス：モニターするように設定されたブロックリスト（セキュリティ インテリジェンス イベントも生成されます）
- SSL ルール：[モニター（Monitor）] アクション

- アクセス コントロール ルール：[モニタ（Monitor）] アクション

システムは、1 つの接続が 1 つのモニタ ルールに一致するたびに 1 つの別個のイベントを生成するわけではありません。1 つの接続が複数のモニタ ルールに一致する可能性があるため、各接続イベントには、接続が一致する最初の 8 つのモニタ アクセス コントロール ルールに関する情報だけでなく、最初の一致する SSL モニタ ルールに関する情報を含めて表示することができます。

同様に、外部 syslog または SNMP トラップ サーバーに接続イベントを送る場合、システムは 1 つの接続が 1 つのモニター ルールに一致するたびに 1 つの別個のアラートを送信するわけではありません。代わりに、接続の終了時にシステムから送られるアラートに、接続が一致したモニター ルールの情報が含まれます。

信頼されている接続のロギング

信頼されている接続の開始と終了をロギングできます。ロギングには、以下のルールとアクションに一致するトラフィックを含めることができます。

- アクセス コントロール ルール：[信頼する（Trust）] アクション
- アクセス コントロールのデフォルト アクション：[すべてのトラフィックを信頼する（Trust All Traffic）]

（注） 信頼できる接続を記録することはできますが、これはお勧めしません。信頼できる接続はディープインスペクションまたは検出の対象ではないため、信頼できる接続の接続イベントに含まれる情報は限定的であるためです。

信頼ルールによって最初のパケットで検出された TCP 接続は、接続終了イベントだけを生成します。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。

ブロックされた接続のロギング

ブロックされた接続をロギングできます。ロギングには、以下のルールとアクションに一致するトラフィックを含めることができます。

- トンネル ルール：[ブロック（Block）]
- プレフィルタ ルール：[ブロック（Block）]
- プレフィルタのデフォルト アクション：[すべてのトンネル トラフィックをブロック（Block all tunnel traffic）]
- セキュリティ インテリジェンス：モニターするように設定されていないブロックリスト（セキュリティ インテリジェンス イベントも生成されます）
- 復号ルール：[ブロック（Block）] および [リセットしてブロック（Block with reset）]

- SSL のデフォルト アクション：[ブロック（Block）]および[リセットしてブロック（Block with reset）]
- アクセス コントロール ルール：[ブロック（Block）]、[リセットしてブロック（Block with reset）]、[インタラクティブ ブロック（Interactive Block）]
- アクセス コントロールのデフォルト アクション：[すべてのトラフィックをブロック（Block All Traffic）]

トラフィックをブロックできるデバイスは、インライン（つまり、ルーテッドインターフェイス、スイッチド インターフェイス、トランスペアレント インターフェイス、インライン インターフェイスのペア）で展開されているもののみです。ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。

注意 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。

ブロックされた接続の接続開始ロギングと接続終了ロギングとの比較

ブロックされた接続をロギングするときは、システムがその接続をどのようにロギングするかは接続がブロックされた理由によって異なります。これは、接続ログに基づいて相関ルールを設定する際に留意しておくことが重要です。

- 暗号化されたトラフィックをブロックする復号ルールおよび復号ポリシーのデフォルト アクションの場合、システムは接続**終了**イベントをロギングします。これは、システムが接続がセッション内で最初のパケットを使用して暗号化されているかどうかを決定できないためです。
- 他のブロッキング アクションについては、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。

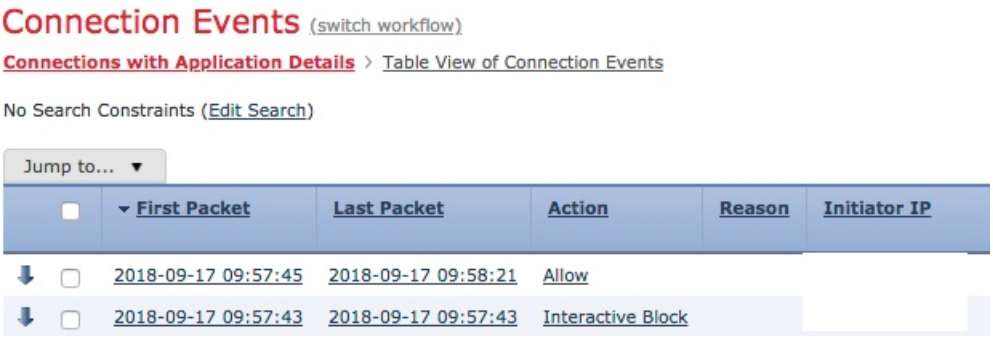
バイパスされるインタラクティブ ブロックのロギング

インタラクティブ ブロッキング アクセス コントロール ルール（このルールではユーザが禁止されている Web サイトを参照するとシステムによって警告ページが表示されます）を使用すると、接続終了ロギングを設定できます。その理由は、警告ページをユーザーがクリック スルーすると、その接続は新規の、許可された接続と見なされ、システムによってモニターとロギングができるためです。

したがって、[インタラクティブ ブロック（Interactive Block）] ルールまたは [リセットしてインタラクティブ ブロック（Interactive Block with reset）] ルールにパケットが一致する場合、システムは以下の接続イベントを生成できます。

- ユーザーの要求が最初にブロックされ警告ページが表示されたときの接続開始イベント。このイベントにはアクション [インタラクティブ ブロック（Interactive Block）] または [リセットしてインタラクティブ ブロック（Interactive Block with Reset）] が関連付けられます。
- 複数の接続開始または終了イベント（ユーザーが警告ページをクリック スルーし、要求した最初のページをロードした場合）。これらのイベントには [許可（Allow）] アクションおよび理由 [ユーザー バイパス（User Bypass）] が関連付けられます。

次の図に、許可を受けたインタラクティブ ブロックの例を示します。



許可された接続のロギング

許可された接続をロギングができます。ロギングには、以下のルールとアクションに一致するトラフィックを含めることができます。

- SSL ルール：[複合（Decrypt）] アクション
- SSL ルール：[複合しない（Do not decrypt）] アクション
- SSL のデフォルト アクション：[複合しない（Do not decrypt）] アクション
- アクセス コントロール ルール：[許可（Allow）] アクション
- アクセス コントロールのデフォルト アクション：[ネットワーク検出のみ（Network Discovery Only）] および任意の侵入防御オプション

これらの設定に対するロギングを有効にすると、接続が確実にロギングされると同時に、インスペクションおよびトラフィック処理の次のフェーズが許可（または指定）されます。SSL ロギングは常に接続終了ロギングですが、アクセス コントロール設定で接続開始ロギングも可能にすることができます。

トンネルおよびプレフィルタ ルールでの [分析（Analyze）] アクションを使用してアクセス コントロールで接続を続行することもできますが、このアクションを使用するルールではロギングが無効にされます。ただし、他の設定を使用して、一致する接続をロギングすることもできます。許可されたトンネルのカプセル化されたセッションは、個別に評価されてロギングされます。

アクセス コントロール ルールまたはデフォルト アクションでトラフィックを許可する場合、関連する侵入ポリシーを使用してトラフィックをさらに検査し、侵入をブロックすることがで

きます。アクセスコントロールルールでは、ファイルポリシーを使用して、マルウェアを含む禁止されたファイルを検出し、ブロックすることもできます。接続イベントストレージを無効にしない限り、システムは、侵入イベント、ファイル イベント、マルウェア イベントに関連する許可された接続のほとんどを自動的にロギングします。詳細については、常にログに記録される接続 （2 ページ）を参照してください。

ペイロードが暗号化される接続には、ディープインスペクションは適用されません。したがって、暗号化接続の接続イベントに含まれる情報は限定されます。

許可された接続のファイルおよびマルウェア イベントのロギング

ファイル ポリシーによってファイルが検出またはブロックされると、以下のいずれかのイベントが Firewall Management Center データベースにロギングされます。

- ファイル イベント：検出またはブロックされたファイル（マルウェア ファイルを含む）を表します。
- マルウェア イベント：検出またはブロックされたマルウェア ファイルのみを表します。
- レトロスペクティブ マルウェア イベント：以前に検出されたファイルでのマルウェア処理が変化した場合に生成されます。

このロギングは、アクセス コントロール ルールごとに無効にすることができます。ファイル イベントおよびマルウェア イベント ストレージを完全に無効にすることもできます。

（注） ファイル イベントおよびマルウェア イベントのロギングは有効のままにすることを推奨しています。

接続開始のロギングと終了のロギングの比較

接続は、次の例外となるブロックされたトラフィックを除き、接続開始時あるいは終了時にログを記録することができます。

- ブロックされたトラフィック：ブロックされたトラフィックは、さらに検査されることなくすぐさま拒否されるため、通常、ブロックされたトラフィックについては、接続開始イベントのみ記録可能です。ログに記録される個々の接続終了はありません。
- ブロックされた暗号化トラフィック：復号ポリシーで接続のロギングを有効にすると、システムは接続開始イベントではなく接続終了イベントをログに記録します。これは、システムは接続がセッション内で最初のパケットを使用して暗号化されているかどうかを判定できず、暗号化されたセッションを即座にブロックできないためです。

パフォーマンスを最適化するためには、接続の開始と終了の両方ではなく、どちらか一方をロギングします。何らかの理由で接続をモニタリングすると、接続終了ロギングが強制されます。単一のブロックされていない接続の場合、接続終了イベントには、接続開始イベントに含まれるすべての情報に加えて、セッション期間中に収集された情報も含まれます。

次の表では、接続開始イベントと接続終了イベントの違い（それぞれをロギングする利点を含む）を詳細に説明します。

表 *1*: 接続開始イベントと接続終了イベントの比較

	接続開始イベント	接続終了イベント
次の場合に生成可能です	システムが接続の開始を検出した場合（または、イベントの生成がアプリケーションまたはURLの識別に依存する場合は最初の数パケットの後）。	システムが以下の状態の場合 • 接続のクローズを検出した場合。 • 一定期間後に接続の終了を検出しない場合。 • メモリ制約によりセッションを追跡できなくなった場合。
次のものについてロギングが可能です	復号ポリシーによってブロックされた接続を除くすべての接続。	ほとんどの接続。
次を含みます	最初のパケット（または、イベントの生成がアプリケーションまたはURLの識別に依存する場合は最初の数パケット）で判定できる情報のみ。	接続開始イベント内のすべての情報と、セッション期間を通してトラフィックを検査して判別された情報（たとえば伝送されたデータ総量、接続の最後のパケットのタイムスタンプなど）。 （注） 接続イベントでは、脅威防御が接続のSnort判定を返した後に、または接続を高速パス処理した場合に、送信されたデータの量がカウントされません。
次の場合に有用です	ログに記録する場合： • ブロックされている接続。 • 接続終了情報はユーザーにとって重要ではないので、接続の開始のみ。	目的 • 復号ポリシーによって処理される暗号化接続をロギングする場合。 • セッションの期間にわたって収集された情報であらゆる種類の詳細な分析を実行する場合、またはその情報を使用して相関ルールをトリガーする場合。 • カスタムワークフローで接続の概要（集約接続データ）を表示する場合、グラフ形式で接続データを表示する場合、またはトラフィックプロファイルを作成して使用する場合。

Secure Firewall Management Center と外部ロギング

接続およびセキュリティ インテリジェンス イベント ログを Firewall Management Center に保存する場合、システムのレポート、分析、およびデータ相関機能を使用することができます。次に例を示します。

- ダッシュボードおよびコンテキストエクスプローラでは、システムによってロギングされた接続をグラフ形式によって一目で確認できます。
- イベント ビュー（ほとんどのオプションは分析メニューで利用可能）には、システムが記録した接続に関する詳細情報が表示されます。これらの情報はグラフまたは表形式で表示したり、レポートにまとめたりすることもできます。
- トラフィック プロファイリングは、接続データを使用して正常なネットワーク トラフィックのプロファイルを作成します。ユーザーはそのプロファイルを基準として使用して、異常な動作を検出および追跡できます。
- 相関ポリシーを使用して、イベントを生成し、特定のタイプの接続またはトラフィック プロファイルの変更に対する応答（アラートや外部修復など）をトリガーできます。

Firewall Management Center に保存できるイベントの数はモデルによって異なります。

（注） これらの機能を使用するには、接続（ほとんどの場合、接続の開始ではなく接続の終了）をロギングする**必要があります**。システムがクリティカルな接続（ログに記録された侵入、禁止されたファイルおよびマルウェアに関連付けられているもの）を自動的にロギングするのはこのためです。

次を使用して、外部の syslog、SNMP トラップサーバー、またはその他の外部ツールにイベントを記録することもできます。

- 任意のデバイスでの外部ロギングの場合：

  設定する接続は、アラート応答と呼ばれます。

- Firewall Threat Defense デバイスでの外部ロギングの場合：

  Cisco Secure Firewall Management Center デバイス構成ガイドの「*About Configuring Syslog*」および「*Configure SNMP Traps*」を参照してください。

- 外部ロギングに関連するその他のオプションの場合：

  「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。

関連トピック

Secure Firewall Management Center アラート応答

接続ロギングの制限事項

以下はロギングできません。

- カプセル化された接続がアクセス制御によって検査されるプレーンテキスト、パススルートンネルの外部セッション。
- 3 ウェイ ハンドシェイクが完了していない場合の TCP 接続 。ファイアウォールに対するサービス拒否攻撃を回避します。失敗した接続をモニターまたはデバッグするには、**show asp drops** CLI コマンドまたはパケットキャプチャ機能（パケット キャプチャの概要）を使用できます。

接続イベントに必要と思われる情報が含まれていない場合は、接続イベント フィールドの入力の要件と接続イベント フィールドで利用可能な情報を参照してください。

イベント ビューアにイベントが表示された場合

次のポイントは、すべてのタイプのイベントに適用されます。

- [分析 (Analysis)] メニューの下にあるページを見ている場合は、ページを更新して新しいイベントを表示する必要があります。
- 通常、イベントは、トラフィックが検出されてから数秒以内に表示されます。ただし、トラフィックが非常に多い状態、FMC が低帯域幅のネットワーク上で多数のデバイスを管理している状況、またはイベントのバックアップなどのイベント処理が一時停止される操作が進行中である状況などでは、任意の遅延が生じることがあります。
- 定義されたルールに従って記録されたすべての接続イベントが、イベントビューアに表示されます。イベントをフィルタするオプションは、接続イベントの統合ロギングには使用できません。

接続のロギングのベスト プラクティス

次のベスト プラクティスを使用して、記録が必要な接続のみを記録するようにします。

重要な接続のみが記録されるように、アクセス制御ルールごとの接続ロギングを有効にします。

常に記録する接続

システムは次について自動的に記録します。

- 検出されたファイル、マルウェア、侵入、およびインテリジェント アプリケーション バイパス（IAB）に関連付けられている一部の接続。

  詳細については、常にログに記録される接続 （2 ページ）を参照してください。

- モニター対象の接続。

  詳細については、モニターされた監視接続のロギング （4ページ）を参照してください。

記録されることがない接続

次についてはロギングを有効にしないでください。

- 信頼アクションがあるアクセス制御ルール

  信頼されている接続には、ディープインスペクションまたはディスカバリは適用されません。したがって、信頼されている接続の接続イベントに含まれる情報は限られます。

- パッシブ展開のブロック ルールについてはロギングを有効にしないでください。デバイスがインラインで展開された場合にシステムがブロックする接続を記録するには、ブロック ルールではなく、モニター ルールを使用します。

  トラフィックをブロックできるデバイスは、インライン（つまり、ルーテッド インターフェイス、スイッチド インターフェイス、トランスペアレント インターフェイス、インライン インターフェイスのペア）で展開されているもののみです。ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。

- 対象外のトラフィック。次に例を示します。

  - 信頼されている DNS ホストへの DNS 要求などの特定の許可トラフィック。
  - サービス提供に関係のないインフラストラクチャ トラフィック。

  （前述のように、この場合もこのトラフィックの脅威はモニターできます。）

常にログに記録される接続 （2 ページ）で説明したように、前述のロギングを無効にした場合も、侵入イベント、マルウェア、および IAB は記録されます。

どこかで記録されているものの記録の回避

別のデバイスまたはサービスがネットワークセグメントの接続データを記録している場合は、Firewall Management Center 内のそのセグメントのデータのロギングを無効にします。次に例を示します。

- Firewall Management Center と同じネットワークセグメント上の接続イベントをルータが記録している場合、相関ポリシーやトラフィックプロファイルなど何らかの目的で接続イベントが必要な場合を除き、Firewall Management Center 上での同じ接続を記録することは避けてください。

  相関ポリシーの詳細については、相関ポリシーとルールの概要を参照してください。トラフィック プロファイルの詳細については、トラフィック プロファイルの概要を参照してください。

- Secure Network Analytics を使用してスイッチやルータから報告された NetFlow レコードを利用して潜在的な動作の異常や疑わしいトラフィックパターンを特定している場合、それらのセグメントをモニターしているルールの接続ロギングを無効することができます。そ

の代りに、ネットワークのそれらの部分については Secure Network Analytics の動作分析に依存します。

詳細については、Secure Network Analytics のドキュメントを参照してください。

接続の開始または終了のいずれか（両方ではない）のロギング

接続の開始と終了のロギングを選択できる場合は、接続終了時のロギングを有効にします。これは、接続終了時は接続開始イベントからの情報と、セッション中に収集された情報が記録されるからです。

ブロックされた接続を記録するか、または接続終了の情報に関心がない場合にのみ、接続の開始を記録します。

詳細については、接続開始のロギングと終了のロギングの比較 （8 ページ）を参照してください。

ブロックされたトラフィックのロギング

ブロックされたトラフィックは、それ以上調査されることなくすぐに拒否されるため、通常は接続開始イベントのみを記録できます。

詳細については、ブロックされた接続のロギング （5 ページ）を参照してください。

外部の場所へのイベントのロギング

会社のセキュリティポリシーで許可されている場合は、次のいずれかを使用して外部ソースにログをストリーミングすることで Firewall Management Center のディスク容量を節約できます。

- eStreamer は、Firewall Management Center あるいは からカスタム展開したクライアント アプリケーションへのログのストリーミングを可能にします。詳細については、『*Secure Firewall Management Center Event Streamer Integration Guide*』と『』[英語] を参照してください。
- アラート応答と呼ばれている syslog または SNMP トラップ。詳細については、Secure Firewall Management Center アラート応答を参照してください。

イベント レコードの最大数を指定します。

データベースに保存できるレコードの最小数と最大数を考慮します。たとえば、デフォルトでは、仮想 Firewall Management Center は 1,000 万のイベントを保存できますが、イベントの最大数は 5,000 万です。**[システム（System）] > [設定（Configuration）] > [データベース（Database）]** に移動してニーズに合ったサイズに調整します。

Firewall Management Center のすべてのモデルとそれらのイベントデータベースのサイズのリストについては、データベース イベント数の制限 を参照してください。

接続イベントに表示される内容を制御します。

接続イベントに表示される行数を指定するには、Firewall Management Center の右上にある自分のユーザー名をクリックし、**[ユーザー設定（User Preferences）] > [イベント表示設定（Event View Settings）]** をクリックします。設定可能なイベント数は 1 ページあたり最大で 1,000 です。

接続イベント レポートのセットアップ

接続イベントを見逃していないことを確認するには、.csv 形式の自動レポートをセットアップし、必要に応じて定期的に実行されるようにスケジュールを設定することができます。詳細については、次のトピックを参照してください。

- レポートデザイナを使用します（**[分析（Analysis）] > [接続（Connection）] > [イベント（Events）] > [レポートデザイナ（Report Designer）]**）。レポートの設計について
- タスクのスケジュールを設定します（**[システム（System）] > [ツール（Tools）] > [スケジュール（Scheduling）]**）。タスクのスケジューリングについて

接続ロギングの要件と前提条件

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
- アクセス管理者
- ネットワーク管理者

接続ロギングの設定

以降の項では、さまざまなルールと条件に一致する接続ロギングのセットアップ方法について説明します。

トンネル ルールおよびプレフィルタ ルールによる接続のロギング

プレフィルターポリシーは Secure Firewall Threat Defense デバイスにのみ適用されます。

始める前に

- ルール アクションを [ブロック（Block）] または [ファストパス（Fastpath）] に設定します。[分析（Analyze）]アクションのロギングは無効にします。これにより、接続のアクセス制御が引き続き可能になり、接続の処理とロギングは別の設定で決定されます。
- ロギングは、カプセル化フローではなく、内部フローで実行されます。

手順

ステップ 1 プレフィルタポリシーエディタで、ロギングを設定するルールの横にある [編集（Edit）]（✎）をクリックします。

代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 2 [ロギング（Logging）] をクリックします。

ステップ 3 [接続の開始時にロギングする（Log at Beginning of Connection）] または [接続の終了時にロギングする（Log at End of Connection）] を指定します。

パフォーマンスを最適化するためには、接続の開始と終了の両方ではなく、どちらか一方をロギングします。ブロックされたトラフィックは、それ以上の検査なしで即座に拒否されるため、[ブロック（Block）] ルールの場合は接続終了時のイベントはロギングできません。

ステップ 4 接続イベントの送信先を指定します。

ステップ 5 [保存（Save）] をクリックしてルールを保存します。

ステップ 6 [保存（Save）] をクリックして、プレフィルタポリシーを保存します。

次のタスク

- 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

TLS/SSL復号ルールを使用した復号可能接続のロギング

手順

ステップ 1 復号ポリシーエディタで、ロギングを設定するルールの横にある [編集（Edit）]（✎）をクリックします。

代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 2 [ロギング（Logging）] をクリックします。

ステップ 3 **[接続終了時にロギング（Log at End of Connection）]** チェックボックスをオンにします。

モニター対象トラフィックに対して、接続の終了時のロギングが必要になります。

ステップ 4 接続イベントの送信先を指定します。

接続イベントについてFirewall Management Centerベースの分析を実行する場合は、イベントをイベント ビューアに送信します。モニター対象トラフィックに対して、これが必要になります。

ステップ 5 [保存（Save）] をクリックしてルールを保存します。

ステップ 6 **[保存（Save）]** をクリックして、復号ポリシーを保存します。

次のタスク

- 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

セキュリティ インテリジェンスを使用した接続のロギング

セキュリティ インテリジェンス ポリシーには、脅威スマート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 エディタで、[セキュリティ インテリジェンス（Security Intelligence）] をクリックします。

ステップ 2 **ロギング**（） アイコンをクリックし、次の基準を使用してセキュリティ インテリジェンス ロギングを有効にします。

- IP アドレス別：[ネットワーク（Networks）] の横にあるロギング アイコンをクリックします。
- URL 別：[URL（URLs）] の横にあるロギング アイコンをクリックします。
- ドメイン名別：[DNS ポリシー（DNS Policy）] ドロップダウンリストの横にあるロギング アイコンをクリックします。

ロギングアイコンが無効になっている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 3 [接続のロギング（Log Connections）] チェックボックスをオンにします。

ステップ 4 接続先およびセキュリティ関連の接続イベントを指定します。

Firewall Management Centerベースの分析を実行する場合や、ブロックリストをモニター専用に設定する場合は、イベントをイベントビューアに送信します。

ステップ 5 [OK] をクリックしてロギング オプションを設定します。

ステップ 6 [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

- 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

アクセス制御ルールによる接続のロギング

ルール アクションと詳細検査のオプションの選択によって、ロギング オプションは異なります。ルールとポリシーのアクションによるロギングへの影響 （4 ページ）を参照してください。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、ロギングを設定するルールの横にある[編集（Edit）]（✎）をクリックします。

代わりに [表示（View）]（👁） が表示される場合、設定は先祖ポリシーから継承されるか、または先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 2 **[ロギング（Logging）]** をクリックします。

ステップ 3 [接続の開始時にロギングする（Log at Beginning of Connection）] または [接続の終了時にロギングする（Log at End of Connection）] を指定します。

パフォーマンスを最適化するためには、接続の開始と終了の両方ではなく、どちらか一方をロギングします。

ステップ 4 （オプション）[ファイルのロギング（Log Files）] チェックボックスをオンにして、接続に関連付けられているファイル イベントとマルウェア イベントをロギングします。

このオプションは有効のままにすることを推奨します。

ステップ 5 接続イベントの送信先を指定します。

- [イベントビューア（Event Viewers）]：Firewall Management Center にイベントを送信します。クラウド管理を使用している場合、イベント分析のみを実行するように設定しているときは、クラウド提供型 Firewall Management Center およびオンプレミス Firewall Management Center にイベントを送信します。どちらの製品のイベントビューアでもイベントを表示できます。
- [Syslog サーバー（Syslog Server）]：オーバーライドする場合を除き、アクセス コントロール ポリシーに設定されている syslog サーバーに接続イベントを送信します。

[オーバーライドの表示（Show Overrides）]：アクセス コントロール ポリシーで設定されている設定をオーバーライドするためのオプションが表示されます。

- [重大度をオーバーライドする（Override Severity）]：このオプションを選択し、ルールの重大度を選択した場合は、このルールの接続イベントはアクセス コントロール ポリシーの [ロギング（Logging）] タブに設定されている重大度に関わらず、選択した重大度が設定されます。
- [デフォルトの Syslog の宛先をオーバーライドする（Override Default Syslog Destination）]：このルールの接続イベントに生成された syslog をこのアラートに指定されている宛先に送信します。

- [SNMP トラップ（SNMP Trap）]：接続イベントは、選択した SNMP トラップに送信されます。

ステップ 6 [確認（Confirm）] をクリックします。

ステップ 7 **[適用（Apply）]** をクリックして、ルールを保存します。

次のタスク

- 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

ポリシーのデフォルト アクションによる接続のロギング

ポリシーのデフォルトアクションにより、システムがポリシー内のルールのいずれにも一致しないトラフィックを処理する方法が決定されます（ただし、トラフィックの照合およびロギングを実行し、トラフィックの処理や調査は実行しないアクセス コントロール ポリシーと復号ポリシー内のモニタールールを除きます）。

また、システムが複号できないセッションをロギングする方法は、復号ポリシーのデフォルトアクションのロギング設定でも制御されます。

始める前に

- プレフィルタのデフォルトアクション ロギングについては、デフォルトアクションを [すべてのトンネル トラフィックをブロック（Block all tunnel traffic）] に設定します。[すべてのトンネル トラフィックを許可（Allow all tunnel traffic）] アクションのロギングは無効になります。これにより、接続のアクセス制御が引き続き可能になり、接続の処理とロギングは別の設定で決定されます。

手順

ステップ 1 ポリシーエディタで、[デフォルトアクション（Default Action）] ドロップダウンリストの横にある **[デフォルトのロギングおよびインスペクション（Default Logging and Inspection）]** をクリックします。

ステップ 2 一致する接続をロギングするタイミングを指定します。

- 接続の開始時にロギングする：SSL のデフォルト アクションではサポートされていません。
- 接続の終了時にロギングする：アクセス制御の [すべてのトラフィックをブロック（Block All Traffic）] デフォルト アクションまたはプレフィルタの [すべてのトンネル トラフィックをブロック（Block all tunnel traffic）] デフォルト アクションを選択するとサポートされなくなります。

パフォーマンスを最適化するためには、接続の開始と終了の両方ではなく、どちらか一方をロギングします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。アクセス コントロール ポリシーでは、設定が先祖ポリシーから継承されることもあります。

ステップ 3 接続イベントの送信先を指定します。

接続イベントについて Firewall Management Center ベースの分析を実行する場合は、イベントをイベント ビューアに送信します。

ステップ 4 [OK] [適用（Apply）] をクリックします。

ステップ 5 [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

- 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

長い URL のロギング制限

HTTP トラフィックの接続の終了イベントは、監視対象ホストによって要求された URL を記録します。URL の保管を無効にすることや保管する URL 文字数を制限することで、システム パフォーマンスが向上する可能性があります。URL のロギングを無効化しても（保管する文字数を 0 にしても）、URL フィルタリングには影響しません。システムは、要求された URL に基づいてトラフィックをフィルタリングします。それらの URL を記録しない場合も同じです。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、**[その他（More）] > [詳細設定（Advanced Settings）]** をクリックして、[一般設定（General Settings）] の横にある [編集（Edit）]（） をクリックします。

代わりに [表示（View）]（） が表示される場合、設定は先祖ポリシーから継承されるか、または先祖ドメインに属しており、設定を変更する権限がありません。設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 2 [接続イベントで保存する URL の最大文字数（Maximum URL characters to store in connection events）] を入力します。

ステップ 3 [OK] をクリックします。

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

- 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

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。