ネットワーク トラフィックの接続のロギング

デバイスがネットワーク上でホストによって生成されたトラフィックをモニタするとき、デバイスは検出した接続のログを生成できます。アクセス コントロールおよび SSL ポリシーでさまざまな設定を行うことで、ロギングする接続の種類、接続をロギングする時期、およびデータを保存する場所をきめ細かく制御することができます。また、アクセス コントロール ルールの特定のロギング設定では、接続に関連するファイル イベントとマルウェア イベントをログに記録するかどうかも決定します。

ほとんどの場合、接続の開始時および終了時に接続をログに記録できます。接続をログに記録すると、システムによって接続イベントが生成されます。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ラックリスト登録（ブロック）される場合は、セキュリティ インテリジェンス イベントと呼ばれる特別な種類の接続イベントをログに記録することもできます。

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が含まれています。

組織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。

どの接続をログに記録するかの決定

ライセンス：任意

アクセス コントロール ポリシーと SSL ポリシーのさまざまな設定を使用して、ASA FirePOWER モジュールがモニタする接続をログに記録できます。ほとんどの場合、接続の開始時および終了時に接続をログに記録できます。ただし、ブロックされたトラフィックは追加の検査なしですぐに拒否されるため、システムがログに記録できるのはブロックまたはブラックリスト登録

されたトラフィックの接続開始イベントだけです。ログに記録できる固有の接続終了イベントはありません。

接続イベントをログに記録すると、イベント ビューアで表示できます。または、外部 syslog あるいは SNMP トラップ サーバに接続データを送信できます。

ヒント ASA FirePOWER モジュールを使用して接続データの詳細な分析を実行するために、 シスコではクリティカルな接続の終了をログに記録することを推奨しています。

クリティカルな接続のロギング

ライセンス：任意

組織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。目標が生成するイベントの数を抑えパフォーマンスを向上させることである場合は、分析のために重要な接続のロギングのみを有効にします。しかし、プロファイリングの目的でネットワーク トラフィックの広範な表示が必要な場合は、追加の接続のロギングを有効にできます。アクセス コントロールおよび SSL ポリシーでさまざまな設定を行うことで、ロギングする接続の種類、接続をロギングする時期、およびデータを保存する場所をきめ細かく制御することができます。

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、類似の複数のイベントによってシステムが過負荷になる可能性があります。ブロック ルールに対して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。

設定するロギングに加えて、システムは禁止されたファイル、マルウェア、または侵入の試みを検出した場合に、ほとんどの接続を自動的にログに記録します。システムはこれらの接続終了イベントを、さらに分析するために保存します。すべての接続イベントは、自動的にログ記録された理由を [Action] および [Reason] フィールドで反映します。

セキュリティ インテリジェンス ブラックリスト登録の決定（オプション）

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ラックリスト登録（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、ブラックリスト登録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、ブラックリストと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 ロギングを有効にすると、ブラックリストの一致によってセキュリティ インテリジェンス イベントおよび接続イベントが生成されます。セキュリティ インテリジェンス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できるだけ

でなく、個別に保存およびプルーニングできます。詳細については、セキュリティ インテリジェンス（ブラックリスト登録）の決定のロギング （9 ページ）を参照してください。

アクセス コントロールの処理（任意）

接続がアクセス コントロール ルールまたはアクセス コントロールのデフォルト アクションによって処理される場合は、その接続をログに記録できます。このロギングはアクセス コントロール ルールごとに設定し、クリティカルな接続のみをログに記録できるようにします。詳細については、アクセス コントロールの処理に基づく接続のロギング （11 ページ）を参照してください。

侵入に関連付けられた接続（自動）

アクセス コントロール ルールによって呼び出された侵入ポリシー（アクセス コントロール ルールを使用したトラフィック フローの調整を参照）が侵入を検出して侵入イベントを生成すると、システムはルールのロギング設定に関係なく、侵入が発生した接続の終了を自動的にロギングします。

しかし、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（デフォルトの処理の設定およびネットワーク トラフィックのインスペクションを参照）によって侵入イベントが生成された場合、システムは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。

侵入がブロックされた接続では、接続ログ内の接続のアクションは Block、理由は Intrusion Block ですが、侵入インスペクションを実行するには、許可ルールを使用する必要があります。

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（自動）

アクセス コントロール ルールによって呼び出されたファイル ポリシーが禁止されたファイル（マルウェアを含む）を検出してファイル イベントまたはマルウェア イベントを生成すると、システムはアクセス コントロール ルールのロギング設定に関係なく、ファイルが検出された接続の終了をデータベースに自動的にロギングします。このロギングを無効にすることはできません。

（注） NetBIOS-ssn（SMB）トラフィックの検査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。

ファイルがブロックされた接続では、接続ログ内の接続のアクションは [ブロック（Block）] ですが、ファイルおよびマルウェアのインスペクションを実行するには、許可ルールを使用する必要があります。接続の原因は、File Monitor（ファイル タイプまたはマルウェアが検出された）、あるいは Malware Block または File Block（ファイルがブロックされた）です。

接続の開始および終了のロギング

ライセンス：任意

システムが接続を検出すると、ほとんどの場合、その開始および終了をログに記録できます。

ただし、ブロックされたトラフィックは追加の検査なしですぐに拒否されるため、多くの場合、ユーザがログに記録できるのはブロックまたはブラックリスト登録されたトラフィックの接続開始イベントだけです。ログに記録できる固有の接続終了イベントはありません。

（注） 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。

何らかの理由で接続をモニタすると、接続終了ロギングが強制されることに注意してください。モニタされる接続のロギングについて （5 ページ） を参照してください。

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。

コンテキスト	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	セキュリティ インテリジェンスまたはアクセス コントロール ルールで評価されているすべての接続	すべての接続は構成可能。ただしシステムはブロックされている接続またはブラックリストに登録されている接続の終わりをログに記録できない。
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）で判別できる情報のみ	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）

コンテキスト	接続開始イベント	接続終了イベント
次の場合に有用です	次のものをロギングする場合 • セキュリティ インテリジェンス ブラックリスト登録の決定を含む、ブロックされた接続	次を実行する場合 • 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 • グラフィカル形式での接続データの表示

ASA FirePOWER モジュールまたは外部サーバへの接続のロギング

ライセンス：任意

接続イベントのログは、ASA FirePOWER モジュールの他に、外部の syslog または SNMP トラップ サーバに記録できます。外部サーバに接続データを記録する前に、そのサーバにアラート応答という接続を設定する必要があります。アラート応答の使用を参照してください。

アクセス コントロールおよび SSL ルール アクションがどのようにロギングに影響を及ぼすかについて

ライセンス：機能に応じて異なる

すべてのアクセス コントロールおよび SSL ルールにはアクションがあり、それによってシステムがルールに一致するトラフィックを検査および処理する方法だけでなく、一致するトラフィックに関する詳細をユーザがロギングできる時期と方法が決まります。

モニタされる接続のロギングについて

ライセンス：機能に応じて異なる

システムは、ルールのロギング設定や、後で接続を処理するデフォルト アクションとは関係なく、次の接続の終了を ASA FirePOWER モジュールに常にロギングします。

- モニタに設定されたセキュリティ インテリジェンスのブラックリストに一致する接続
- アクセス コントロールのモニタ ルールに一致する接続

言い換えると、パケットが他のルールに一致せず、デフォルト アクションでロギングが有効になっていない場合でも、パケットがモニタ ルールまたはセキュリティ インテリジェンスのモニタ対象ブラックリストに一致すれば、必ず接続がロギングされます。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できます。セキュリティインテリジェンス（ブラックリスト登録）の決定のロギング （9 ページ） を参照してください。

モニタ対象のトラフィックは、必ず後で別のルールまたはデフォルトアクションによって処理されるため、モニタ ルールが原因でロギングされる接続に関連するアクションは、決して Monitor にはなりません。代わりに、後で接続を処理するルールまたはデフォルト アクションの操作が反映されます。

システムは、1 つの接続が 1 つの SSL またはアクセス コントロールのモニタ 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、ASA FirePOWER モジュールにロギングされる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、最初に一致するモニタ SSL ルールに関する情報を含めて表示できます。

同様に、外部 syslog または SNMP トラップ サーバ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 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 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について

ライセンス：機能に応じて異なる

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。これらの接続の開始と終了をロギングできますが、暗号化されているかどうかにかかわらず、信頼されている接続は、侵入や、禁止されているファイルおよびマルウェアについて検査されないことに注意してください。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。

ブロックされた接続およびインタラクティブにブロックされた接続のロギングについて

ライセンス：機能に応じて異なる

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（インタラクティブなブロッキング ルールを含む）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。

アクセス コントロールまたは SSL ルールでブロックされたセッションの接続イベントには、Block または Block with reset アクションがあります。ブロックされた暗号化接続の理由は SSL Block です。

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（禁止されている Web サイトをユーザが参照するとシステムによって警告ページが表示される）は、接続の終了をログに記録します。その理由は、警告ページをユーザがクリック 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とロギングができるためです。許可された接続のロギングについて （7 ページ） を参照してください。

したがって、インタラクティブ ブロック ルールまたはリセット付きインタラクティブ ブロック 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Allowアクションおよび理由 User Bypass が関連付けられます）

インラインで展開されたデバイスのみがトラフィックをブロックできることに注意してください。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、類似の複数のイベントによってシステムが過負荷になる可能性があります。ブロック ルールに対して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。

許可された接続のロギングについて

ライセンス：機能に応じて異なる

[復号（Decrypt）] SSL ルール、[復号しない（Do not decrypt）] SSL ルール、および [許可（Allow）]アクセス コントロール ルールは、一致するトラフィックを許可し、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へと通過させます。

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、トラフィックをさらに検査し、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。

許可アクセス コントロール ルールに一致するトラフィックの接続は次のようにロギングされます。

- アクセス コントロール ルールによって呼び出された侵入ポリシーが侵入を検出して侵入イベントを生成すると、システムはルールのロギング設定に関係なく、侵入が発生した接続の終了を ASA FirePOWER モジュールに自動的にロギングします。
- アクセス コントロール ルールによって呼び出されたファイル ポリシーが禁止されたファイル（マルウェアを含む）を検出してファイル イベントまたはマルウェア イベントを生成すると、システムはアクセス コントロール ルールのロギング設定に関係なく、ファイルが検出された接続の終了を ASA FirePOWER モジュールに自動的にロギングします。
- 任意で、システムが安全と見なすトラフィックや、侵入ポリシーまたはファイル ポリシーで検査をしないトラフィックなど、許可されたトラフィックに対して接続の開始および終了のロギングを有効にできます。

結果として生じるすべての接続イベントで、[Action] および [Reason] フィールドにイベントがロギングされた理由が反映されます。次の点に注意してください。

- アクション Allow は、最終宛先に到達した明示的に許可され、ユーザがバイパスしたインタラクティブにブロックされた接続を表します。
- アクション Block は、アクセス コントロール ルールによって初めは許可されたが、侵入、禁止されたファイル、またはマルウェアが検出された接続を表します。

許可された接続のファイルおよびマルウェア イベント ロギングの無効化

ライセンス：Protection または Malware

アクセス コントロール ルールで暗号化されていないまたは復号化されたトラフィックを許可すると、関連付けられたファイル ポリシーを使用して、送信されたファイルを検査し、そのトラフィックが宛先に到達する前に禁止されたファイルおよびマルウェアをブロックできます。侵入防御パフォーマンスの調整を参照してください。

システムは禁止されたファイルを検出すると、次のタイプのイベントの 1 つを ASA FirePOWER モジュールに自動的にロギングします。

- 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に関するマルウェアの性質が変化した場合に生成されます。

ファイル イベントまたはマルウェア イベントをロギングしない場合は、アクセス コントロール ルール エディタの [Logging] タブの [Log Files] チェックボックスをオフにすることで、アクセス コントロール ルールごとにロギングを無効にできます。

（注） Cisco では、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を有効のままにすることを推奨しています。

ファイル イベントおよびマルウェア イベントを保存するかどうかに関係なく、ネットワーク トラフィックがファイル ポリシーに違反すると、呼び出し元のアクセス コントロール ルールのロギング設定に関係なく、システムは関連付けられた接続の終了を ASA FirePOWER モジュールに自動的にロギングします。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（自動） （3 ページ）を参照してください。

接続ロギングのライセンス要件

ライセンス：機能に応じて異なる

アクセス コントロール ポリシーおよび SSL ポリシーで接続ロギングを設定する前に、これらのポリシーが正常に処理できる任意の接続をロギングできます。

アクセス コントロール ポリシーおよびSSL ポリシーは、 ASA FirePOWER モジュールのどのライセンスでも作成できますが、アクセスコントロールの一部の操作を行うには、ポリシーを適用する前に、特定のライセンス機能を有効にする必要があります。

次の表では、アクセス コントロールを正常に設定し、アクセス コントロール ポリシーによって処理される接続をロギングするために必要なライセンスについて説明します。

表 *1:* アクセス コントロール ポリシーにおける接続ロギングのライセンス要件

次の接続をロギングするには	ライセンス
ネットワーク、ポート、またはリテラル URL 基準を使用して処理されるトラフィック用	任意
位置情報データを使用して処理されるトラフィック用	任意
関連付ける対象 • レピュテーションが低い IP アドレス（セキュリティ インテリジェンスのフィルタリング） • 暗号化されていないまたは復号化されたトラフィックの侵入または禁止されたファイル	Protection
暗号化されていないまたは復号化されたトラフィックで検出されたマルウェアに関連付けられる	Malware
ユーザ制御またはアプリケーション制御によって処理されるトラフィック用	Control
URL カテゴリおよびレピュテーション データを使用してシステムがフィルタリングするトラフィック用、およびモニタ対象ホストによって要求される URL の URL カテゴリおよび URL レピュテーション情報を表示するため	URL Filtering

セキュリティインテリジェンス（ブラックリスト登録）の決定のロギング

ライセンス：Protection

悪意のあるインターネット コンテンツに対する第一の防衛ラインとして、ASA FirePOWER モジュールにはセキュリティインテリジェンス機能があります。この機能により、最新のレピュテーションインテリジェンスに基づいて接続をただちにブラックリスト登録（ブロック）することができ、リソースを集中的に使用する詳細な分析が不要になります。このトラフィックフィルタリングは、他のどのポリシーベースのインスペクション、分析、またはトラフィック処理よりも前に行われます。

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、ブラックリスト登

録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、ブラックリストと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 インテリジェンスのロギングを有効にすると、アクセス コントロール ポリシーによって処理されるすべてのブロックされた接続およびモニタされた接続がロギングされます。ただし、システムはホワイトリストの一致はロギングしません。ホワイトリストに登録された接続のロギングは、その接続の最終的な傾向によって異なります。

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できます。どちらのタイプのイベントも、[Action]および[Reason]フィールドを使用して、ブラックリストの一致を反映します。さらに、接続でブラックリスト登録された IP アドレスを特定できるように、イベント ビューアで IP アドレスの横にあるホスト アイコンは、ブラックリスト登録された IP アドレスとモニタされた IP アドレスでは少々異なる表示になっています。

ブロックされたブラックリスト登録された接続のロギング

ブロックされた接続の場合、システムは接続開始セキュリティ インテリジェンス イベントと接続イベントをロギングします。ブラックリスト登録されたトラフィックは追加のインスペクションなしですぐに拒否されるため、ログに記録できる固有の接続終了イベントはありません。これらのイベントの場合、アクションは Block で、理由は IP Block です。

IP Block 接続イベントのしきい値は、開始側と応答側の固有のペアあたり 15 秒です。つまり、システムは接続をブロックしてイベントを生成した時点から 15 秒の間、この 2 つのホスト間で接続がブロックされたとしても、ポートやプロトコルの違いに関わらず、別の接続イベントを生成しません。

モニタされブラックリスト登録された接続のロギング

セキュリティインテリジェンスによって（ブロックされるのではなく）モニタされた接続の場合、システムは接続終了セキュリティ インテリジェンス イベントと接続イベントを、ASA FirePOWER モジュールにロギングします。このロギングは、接続が後で SSL ポリシー、アクセス コントロール ルール、またはアクセス コントロールのデフォルト アクションによってどのように処理されるかにかかわらず発生します。

これらの接続イベントの場合、アクションは接続の最終的な傾向によって異なります。[Reason] フィールドには、IP Monitor と、接続がロギングされている可能性がある他の理由が含まれています。

ただし、モニタされる接続の場合、以降に接続を処理するアクセス コントロール ルールやデフォルトアクションでのロギング設定によっては、接続開始イベントが生成されることもあります。

ブラックリスト登録された接続をログに記録する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

[Access Control Policy] ページが表示されます。

ステップ 2 設定するアクセス コントロール ポリシーの横にある編集アイコンをクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3 [Security Intelligence] タブを選択します。

アクセス コントロール ポリシーのセキュリティ インテリジェンス設定が表示されます。

ステップ 4 ロギング アイコンをクリックします。

[Blacklist Options] ポップアップ ウィンドウが表示されます。

ステップ 5 [Log Connections] チェックボックスをオンにします。

ステップ 6 接続イベントとセキュリティ インテリジェンス イベントの送信先を指定します。次の選択肢があります。

- ASA FirePOWER モジュールにイベントを送信するには、[Event Viewer] を選択します。
- イベントを外部 syslog サーバに送信するには、[Syslog] を選択して、ドロップダウンリストから syslog アラート応答を選択します。必要に応じて、追加アイコンをクリックして syslog アラート応答を追加することもできます（Syslog アラート応答の作成を参照）。
- 接続イベントを SNMP トラップ サーバに送信する場合は、[SNMP Trap] を選択し、ドロップダウン リストから SNMP アラート応答を選択します。必要に応じて、追加アイコンをクリックして SNMP アラート応答を追加することもできます（SNMP アラート応答の作成を参照）。

ブラックリスト登録されたオブジェクトをモニタ専用に設定する場合、またはセキュリティ インテリジェンス フィルタリングによって生成された接続イベントで他の ASA FirePOWER モジュール ベースの分析を行う場合は、イベントをイベント ビューアに送信する必要があります。詳細については、ASA FirePOWER モジュールまたは外部サーバへの接続のロギング （5 ページ）を参照してください。

ステップ 7 [OK] をクリックしてロギング オプションを設定します。

[Security Intelligence] タブが再表示されます。

ステップ 8 [Store ASA FirePOWER Changes] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（設定変更の導入を参照してください）。

アクセス コントロールの処理に基づく接続のロギング

ライセンス：任意

アクセス コントロール ポリシー内で、アクセス コントロール ルールはネットワーク トラフィックを処理する詳細な方法を提供しています。クリティカルな接続のみをロギングできるように、アクセス コントロール ルールごとに接続ロギングを有効にします。あるルールに対して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るすべての接続をロギングします。

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トラフィックの接続をログに記録することもできます。デフォルト アクションによって、システムがポリシー

内のアクセス コントロール 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まります（トラフィックに一致しロギングするが、処理または検査はしないモニタ ルールを除く）。

すべてのアクセス コントロール ルールおよびデフォルト アクションのロギングを無効にしても、接続がアクセス コントロール ルールに一致し、侵入の試み、禁止されたファイル、またはマルウェアが含まれている場合、またはシステムによって復号化され、SSL ポリシーで接続のロギングを有効にした場合は、接続終了イベントは引き続き ASA FirePOWER モジュールにロギングされる場合があることに注意してください。

ルールまたはデフォルトのポリシー アクション、および設定した関連するインスペクション オプションによって、ロギング オプションは異なります。

アクセス コントロール ルールに一致する接続のロギング

ライセンス：任意

クリティカルな接続のみをロギングするには、アクセス コントロール ルールごとに接続ロギングを有効にします。あるルールに対し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。

ルール アクションおよびそのルールの侵入およびファイルのインスペクション設定によって、ロギング オプションは異なります。アクセス コントロールおよび SSL ルール アクションがどのようにロギングに影響を及ぼすかについて （5 ページ） を参照してください。また、アクセス コントロール ルールに対してロギングを無効にしても、接続が以下に当てはまる場合は、そのルールに一致する接続の接続終了イベントは引き続き ASA FirePOWER モジュールにロギングされる場合があることに注意してください。

- 侵入の試み、禁止されたファイル、またはマルウェアが含まれている場合
- 以前に少なくとも 1 つのアクセス コントロールのモニタ ルールに一致した場合

接続、ファイル、およびマルウェア情報をログに記録するアクセス コントロール ルールを設定する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] の順に選択します。

[Access Control Policy] ページが表示されます。

ステップ 2 変更するアクセス コントロール ポリシーの横にある編集アイコンをクリックします。

アクセス コントロール ポリシー エディタが表示され、[Rules] タブに焦点が置かれています。

ステップ 3 ロギングを設定するルールの横にある編集アイコンをクリックします。

アクセス コントロール ルール エディタが表示されます。

ステップ 4 [Logging] タブを選択します。

[Logging] タブが表示されます。

ステップ 5 [Log at Beginning and End of Connection]、[Log at End of Connection] を選択して、接続の開始時と終了時または終了時のみにログに記録することを指定するか、または [No Logging at Connection] を選択して、接続時にはログに記録しないことを指定します。

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。ブロックされたトラフィックは追加の検査なしで即座に拒否されるので、ブロック ルールについては接続開始イベントだけがログに記録されます。このため、ルール アクションを [Block] または [Block with reset] に設定すると、**接続の開始時点でロギングを行う**よう指示するプロンプトが表示されます。

ステップ 6 接続に関連しているファイル イベントとマルウェア イベントをすべてログに記録するかどうか指定するには、[Log Files] チェック ボックスを使用します。

ユーザがファイル ポリシーをルールに関連付けてファイル制御または AMP を実行すると、システムはこのオプションを自動的に有効にします。シスコでは、このオプションを有効のままにすることを推奨しています。許可された接続のファイルおよびマルウェア イベント ロギングの無効化 （8 ページ）を参照してください。

ステップ 7 接続イベントの送信先を指定します。次の選択肢があります。

- ASA FirePOWER モジュールに接続イベントを送信するには、[Event Viewer] を選択します。このオプションは、モニタ ルールに対して無効にできません。
- イベントを外部 syslog サーバに送信するには、[Syslog] を選択して、ドロップダウンリストから syslog アラート応答を選択します。必要に応じて、追加アイコンをクリックして Syslog アラート応答を追加することもできます（Syslog アラート応答の作成を参照）。
- イベントを SNMP トラップ サーバに送信するには、[SNMP Trap] を選択し、ドロップダウンリストから SNMP アラート応答を選択します。必要に応じて、追加アイコンをクリックして SNMP アラート応答を追加することもできます（SNMP アラート応答の作成を参照）。

接続イベントで ASA FirePOWER モジュール ベースの分析を実行する場合は、イベントをイベント ビューアに送信する必要があります。詳細については、ASA FirePOWER モジュールまたは外部サーバへの接続のロギング （5 ページ）を参照してください。

ステップ 8 [Store ASA FirePOWER Changes] をクリックしてルールを保存します。

ルールが保存されます。変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（設定変更の導入を参照してください）。

アクセス コントロールのデフォルト アクションによって処理される接続のロギング

ライセンス：任意

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トラフィックの接続をログに記録することができます。デフォルト アクションは、ポリシー内のどのアクセス

コントロールルール（トラフィックの照合とロギングは行うが、処理または検査はしないモニタ ルールを除く）にも一致しないトラフィックをシステムがどのように処理するかを決定します。デフォルトの処理の設定およびネットワーク トラフィックのインスペクション 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って処理された接続のメカニズムとオプションは、次の表で示すように、個々のアクセス コントロール ルールによって処理された接続のロギング オプションとほとんど同じです。つまり、ブロックされたトラフィックを除き、システムは接続の開始と終了をログに記録し、接続イベントを ASA FirePOWER モジュール、または外部の syslog や SNMP トラップ サーバに送信できます。

表 *2:* アクセス コントロールのデフォルト アクションのロギング オプション

デフォルト アクション	比較対象	参照先
Access Control: Block All Traffic	ブロック ルール	ブロックされた接続およびインタラクティブにブロックされた接続のロギングについて （6 ページ）
Access Control: Trust All Traffic	信頼ルール	信頼されている接続のロギングについて （6 ページ）
Intrusion Prevention	関連付けられた侵入ポリシーを持つ許可ルール	許可された接続のロギングについて （7 ページ）

しかし、アクセス コントロール ルールによって処理された接続のロギングとデフォルト アクションによって処理された接続のロギングにはいくつかの違いがあります。

- デフォルト アクションにはファイル ロギング オプションはありません。デフォルト アクションを使用して、ファイル制御または AMP を実行することはできません。
- 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**。このことは、接続データをログに記録する必要がない、侵入検知および侵入防御専用の展開環境に役立ちます。

ただし、デフォルトアクションに対して接続開始および接続終了ロギングを有効にした場合は例外です。この場合、関連付けられた侵入ポリシーがトリガーされると、システムは接続の開始だけでなく、接続の終了もログに記録します。

デフォルトアクションに対してロギングを無効にしても、接続が以前に少なくとも 1 つのアクセス コントロールのモニタ ルールに一致した場合、または SSL ポリシーによって検査およびロギングされた場合は、そのルールに一致する接続の接続終了イベントは引き続き ASA FirePOWER モジュールにロギングされる場合があることに注意してください。

アクセス コントロールのデフォルト アクションによって処理されたトラフィックの接続をログに記録するには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

[Access Control Policy] ページが表示されます。

ステップ 2 変更するアクセス コントロール ポリシーの横にある編集アイコンをクリックします。

アクセス コントロール ポリシー エディタが表示され、[Rules] タブに焦点が置かれています。

ステップ 3 [Default Action] 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。

[Logging] ポップアップ ウィンドウが表示されます。

ステップ 4 [Log at Beginning and End of Connection]、[Log at End of Connection] を選択して、接続の開始時と終了時または終了時のみにログに記録することを指定するか、または [No Logging at Connection] を選択して、接続時にはログに記録しないことを指定します。

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。ブロックされたトラフィックは追加のインスペクションなしで即座に拒否されるので、システムは [Block All Traffic] デフォルト アクションの接続開始イベントのみをログに記録します。このため、デフォルト アクションを [Access Control: Block All Traffic] に設定すると、**接続の開始時点でロギングを行う**よう指示するプロンプトが表示されます。

ステップ 5 接続イベントの送信先を指定します。次の選択肢があります。

- ASA FirePOWER モジュールに接続イベントを送信するには、[Event Viewer] を選択します。このオプションは、モニタ ルールに対して無効にできません。
- イベントを外部 syslog サーバに送信するには、[Syslog] を選択して、ドロップダウンリストから syslog アラート応答を選択します。必要に応じて、追加アイコンをクリックして syslog アラート応答を追加することもできます（Syslog アラート応答の作成を参照）。
- イベントを SNMP トラップ サーバに送信するには、[SNMP Trap]を選択し、ドロップダウンリストから SNMP アラート応答を選択します。必要に応じて、追加アイコンをクリックして SNMP アラート応答を追加することもできます（SNMP アラート応答の作成を参照）。

接続イベントで ASA FirePOWER モジュール ベースの分析を実行する場合は、イベントをイベント ビューアに送信する必要があります。詳細については、ASA FirePOWER モジュールまたは外部サーバへの接続のロギング （5 ページ）を参照してください。

ステップ 6 [Store ASA FirePOWER Changes] をクリックしてポリシーを保存します。

ポリシーが保存されます。変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（設定変更の導入を参照してください）。

接続で検出された URL のロギング

ライセンス：任意

HTTP トラフィックで、接続終了イベントを ASA FirePOWER モジュールにロギングすると、システムはセッション中にモニタ対象ホストにより要求された URL を記録します。

デフォルトでは、システムはURLの最初の1024文字を接続ログに保管します。しかし、モニタ対象のホストが要求する完全なURLが取り込まれるように、URLごとに最大4096文字を保管するようにシステムを設定することができます。または、アクセスされた個々のURLを知る必要がない場合は、保管する文字数をゼロに設定して、URLの保管を無効にすることもできます。ネットワーク トラフィックによっては、URLの保管を無効にするか、あるいは保管するURLの文字数を制限すると、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のロギングを無効にしても、URLフィルタリングには影響しないことに注意してください。アクセスコントロールルールにより、要求されたURL、そのカテゴリ、およびレピュテーションに基づいて、トラフィックが適切にフィルタリングされます。システムが、これらのルールによって処理されたトラフィックで要求された個々のURLを記録しないだけです。詳細については、URLのブロッキングを参照してください。

保存するURLの文字数をカスタマイズするには、次の手順を実行します。

ステップ1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

[Access Control Policy] ページが表示されます。

ステップ2 設定するアクセス コントロール ポリシーの横にある編集アイコンをクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ3 [Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定が表示されます。

ステップ4 [General Settings] の横にある編集アイコンをクリックします。

[General Settings] ポップアップ ウィンドウが表示されます。

ステップ5 **接続イベントで保存するURLの最大文字数**を入力します。

1～4096の値を指定できます。保管する文字数をゼロにすると、URLフィルタリングを無効にすることなくURLの保管が無効になります。

ステップ6 [OK] をクリックします。

アクセス コントロール ポリシーの詳細設定が表示されます。

ステップ7 [Store ASA FirePOWER Changes] をクリックしてポリシーを保存します。

ポリシーが保存されます。変更を反映させるには、アクセスコントロールポリシーを適用する必要があります（設定変更の導入を参照してください）。

暗号化された接続のロギング

ライセンス：任意

アクセス コントロールの一部として、*SSL* インスペクション機能を使用することで、SSL ポリシーを使用してアクセス コントロール ルールによるさらなる評価のために暗号化されたトラフィックを復号化できます。システムがトラフィックを後でどのように処理または検査するかにかかわらず、これらの復号化された接続のログを記録するようにシステムに強制できます。また、暗号化されたトラフィックをブロックするとき、または復号化せずにトラフィックがアクセス コントロール ルールに渡されることを許可するときに、接続をロギングすることもできます。

暗号化セッションの接続ログには、セッションの暗号化に使用される証明書など、暗号化の詳細が含まれます。クリティカルな接続のみをログに記録するように、SSL ポリシーの暗号化されたセッションの接続ロギングは SSL ルールごとに設定します。

SSL ルールを使用した復号可能接続のロギング

ライセンス：任意

SSL ポリシー内では、SSL ルールは複数の管理対象デバイス間で暗号化されたトラフィックを処理する詳細な方法を提供します。クリティカルな接続のみをロギングできるように、SSL ルールごとに接続ロギングを有効にします。あるルールに対して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るすべての接続をロギングします。

SSL ポリシーによって検査される暗号化された接続の場合、接続イベントのログは、外部の syslog や SNMP トラップ サーバに記録できます。ただし次の場合は、接続終了イベントだけをログに記録できます。

- ブロックされた接続（[Block]、[Block with reset]）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（[Monitor]）およびアクセス コントロール ルールに渡す接続（[Decrypt]、[Do not decrypt]）の場合、アクセス コントロール ルールまたはそのセッションを後で処理するデフォルト アクションのロギング設定に関係なく、システムはセッション終了時にイベントを生成します。

詳細については、アクセス コントロールおよび SSL ルール アクションがどのようにロギングに影響を及ぼすかについて （5 ページ）を参照してください。

復号化できる接続をログに記録するには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [SSL] の順に選択します。

[SSL Policy] ページが表示されます。

ステップ 2 ロギングを設定するルールの横にある編集アイコンをクリックします。

SSL ルール エディタが表示されます。

ステップ 3 [Logging] タブを選択します。

[Logging] タブが表示されます。

ステップ 4 [Log at End of Connection] を選択します。

ステップ 5 接続イベントの送信先を指定します。次の選択肢があります。

- イベントを外部の syslog に送信するには、[Syslog] を選択して、ドロップダウンリストから syslog アラート応答を選択します。必要に応じて、追加アイコンをクリックして syslog アラート応答を追加することもできます（Syslog アラート応答の作成を参照）。
- イベントを SNMP トラップ サーバに送信するには、[SNMP Trap]を選択し、ドロップダウンリストから SNMP アラート応答を選択します。必要に応じて、追加アイコンをクリックして SNMP アラート応答を追加することもできます（SNMP アラート応答の作成を参照）。

ステップ 6 [Add] をクリックして変更を保存します。

変更を反映させるには、SSL ポリシーが関連付けられているアクセス コントロール ポリシーを適用する必要があります。設定変更の導入 を参照してください。

暗号化された接続および復号化できない接続のデフォルトのロギング設定

ライセンス：SSL

SSL ポリシーのデフォルト アクションによって処理されるトラフィックの接続をログに記録できます。これらのロギング設定では、システムが復号化できないセッションをどのようにログに記録するかも管理されます。

SSL ポリシーのデフォルト アクションは、ポリシー内のどの SSL ルール（トラフィックの照合とロギングは行うが、処理または検査はしないモニタ ルールを除く）にも一致しない暗号化されたトラフィックをシステムがどのように処理するかを決定します。SSL ポリシーに SSL ルールが含まれていない場合、デフォルト アクションは、ネットワーク上のすべての暗号化セッションがどのようにログに記録されるかを決定します。詳細については、暗号化トラフィックのデフォルトの処理と検査の設定を参照してください。

接続イベントを外部の syslog や SNMP トラップ サーバにロギングするように、SSL ポリシーのデフォルト アクションを設定できます。ただし次の場合は、接続終了イベントだけをログに記録できます。

- ブロックされた接続[Block with reset] の場合、システムは即座にセッションを終了してイベントを生成します。
- 暗号化されていない接続をアクセス コントロールに渡すことを許可する接続の場合（[Do not decrypt]）、システムはセッションの終了時にイベントを生成します。

SSL ポリシーのデフォルト アクションのロギングを無効にしても、接続が以前に少なくとも 1 つの SSL モニタ ルールに一致していた場合、または後でアクセス 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場合は、接続終了イベントが引き続きロギングされる可能性があることに注意してください。

暗号化されたトラフィックおよび復号化できないトラフィックのデフォルトの処理を設定するには、次の手順を実行します。

アクセス：管理者/アクセス管理者/ネットワーク管理者/セキュリティ承認者

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [SSL] の順に選択します。

[SSL Policy] ページが表示されます。

ステップ 2 [Default Action] 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。

[Logging] ポップアップ ウィンドウが表示されます。

ステップ 3 [Log at End of Connection] を選択して、接続イベントのロギングを有効にします。

ステップ 4 接続イベントの送信先を指定します。次の選択肢があります。

- イベントを外部 syslog サーバに送信するには、[Syslog] を選択して、ドロップダウンリストから syslog アラート応答を選択します。必要に応じて、追加アイコンをクリックして syslog アラート応答を設定することもできます（Syslog アラート応答の作成を参照）。
- イベントを SNMP トラップ サーバに送信するには、[SNMP Trap]を選択し、ドロップダウンリストから SNMP アラート応答を選択します。必要に応じて、追加アイコンをクリックして SNMP アラート応答を設定することもできます（SNMP アラート応答の作成を参照）。

ステップ 5 [OK] をクリックして変更を保存します。

変更を反映させるには、SSL ポリシーが関連付けられているアクセス コントロール ポリシーを適用する必要があります。設定変更の導入を参照してください。