CHAPTER 24

Web アプリケーションの保護

このマニュアルでは、Cisco ACE XML ゲートウェイを使用して Web アプリケーションを保護する方法を説明します。内容は次のとおりです。

- 概要
- Web アプリケーション ポリシーのコンポーネント
- Web アプリケーション セキュリティ向けのポリシー作成
- ルールおよび署名の拡張
- メッセージとハンドラの照合
- Web アプリケーションのセキュリティ アクティビティの監視

概要

ACE XML Gateway ではトラフィック処理を設定するうえで、2 つの主要なポリシー オブジェクトである仮想サービスと仮想 Web アプリケーションがあります。

- *仮想サービス*はサービス固有の処理方法をネットワーク トラフィックに適用する際に使用されます。仮想サービスにより、特に XML ベースの通信を統合し保護するのに適した高度な Web サービス機能や他の機能が提供されます。
- *仮想 Web アプリケーション*では、トラフィックの全般的なチェック機能や Web アプリケーションの処理ルールが提供されます。これは、仮想 Web サービスよりも広範な適用設定を対象としており、特に統合作業よりセキュリティに関する作業に的を絞っています。仮想サービスが特定のエンドポイント向けのトラフィック処理志向であるのに対し、仮想 Web アプリケーションは Web アプリケーションに関連するトラフィック クラス全体にわたって処理および検証ルールを幅広く定義しています。

バックエンド Web アプリケーションを保護するには、このアプリケーションに対する仮想 Web アプリケーション オブジェクトをポリシーに作成します。仮想 Web アプリケーションは特定のバックエンド アプリケーションを、アプリケーションのトラフィックに適用する一連のルールと処理手順に関連付けます。要求は、ポリシー内の 1 つの仮想 Web アプリケーションとだけ照合できます。

クライアントが Gateway でプロキシ処理されているアプリケーションにアクセスするには、ポリシー内のアプリケーションに定義されているユーザ インターフェイスに要求を送信します。ACE XML Gateway で仮想 Web アプリケーションまたは仮想サービスのトラフィック フィルタリング基準に合致するトラフィックだけが受け入れられます。それ以外のトラフィックはすべて破棄されます。

ACE XML Gateway はさまざまな方法で要求を検証および処理できます。要求の中に有害となる可能性のあるコンテンツ（潜在的なコマンド インジェクション攻撃またはクロスサイトのスクリプトを書く攻撃を示す文字パターンなど）がないか検索できます。また、HTTP ヘッダーの追加または削除、クッキーの検証、および他のタスクの実行も可能です。

検証および処理されたメッセージは、バックエンド アプリケーションに転送されます。バックエンド アプリケーション側から見ると、ACE XML Gatewayは完全な逆プロキシであるため、アプリケーションは ACE XML Gatewayを要求の発信元と見なします（必要であれば、ACE XML Gatewayは X-Forwarded-For などの HTTP ヘッダーを使用して、バックエンド システムへの実際のメッセージ発信元を識別できます）。ACE XML Gatewayが応答を得ると、機密情報のスクリーニング、クッキーの暗号化、またはエラー応答のマッピングなどを行うことにより、同様に応答をチェックして処理します。

仮想 Web アプリケーション ポリシー オブジェクトは、外部 Web アプリケーション向けのトラフィックの処理方法を決定します。これは次の主要な機能で構成されています。

- ユーザ要求フィルタ。この仮想 Web アプリケーションが処理する着信要求を選択します。
- プロファイル リファレンス。この仮想 Web アプリケーションのトラフィックに適用される検証および処理方法を決定します。
- サーバ リファレンス。発信要求の宛先を決定します。

Cisco ACE XML ゲートウェイのポリシーでは、各仮想 Web アプリケーションの定義は、仮想 Web アプリケーション グループに属します。グループにより、関連する複数の仮想 Web アプリケーションの管理が容易になります。またグループは、目的を記録したり報告するための組織的なユニットとなります。たとえば、Web App Firewall Incidents レポートでは、指定されたグループに該当するイベントだけを表示するよう表示を選別できます。

Web アプリケーション ポリシーのコンポーネント

Web アプリケーション セキュリティに関して Gatewayのポリシーの作成を開始する前に、Web アプリケーションの保護に使用されるポリシー コンポーネントについて十分理解しておく必要があります。

メッセージ ルール

*ルール*とは、メッセージ上で実行される単一チェックを表すポリシー コンポーネントです。ルールによって、チェック対象となるメッセージの各部と、チェックの実行に使用される署名が識別されます。ルールには次の 2 種類あります。

- *メッセージ インスペクション ルール*は、メッセージに特定のコンテンツが含まれていないかをチェックし、合致した場合はメッセージ全体に作用を及ぼします（メッセージをブロックするか、またはイベントを記録したうえでメッセージを通過させます）。この種類のルールは通常、有害なメッセージの識別とブロックに使用されます。
- *コンテンツ上書きルール*は、メッセージ内で合致したコンテンツを置換用の文字に変更します。この種類のルールは、個人情報がバックエンド システムによって不適切に公開されないようにするのに役立ちます。

署名

ルールは、メッセージ コンテンツへの*署名*との照合に基づいて、メッセージに適用されます。署名は、対象となるコンテンツと照合するためメッセージ コンテンツに適用されるパターンです。ルールと同様、署名もグループごとにまとめられています。署名は、数字や文字を含むある決まった文字セットまたは正規表現パターンを使用して、トラフィック コンテンツを照合します。

プロファイル

ルールは Gatewayのトラフィック クラスに対して*プロファイル*ごとに適用されます。プロファイルは、ルールとアクティブ セキュリティ設定で構成される指定された項目の集合です。プロファイルは、プロファイルのコンテキストでどのルール グループが有効になっているか（他のプロファイルではこの

プロファイルと異なり、ルールが有効になっている場合がある）、および設定に対する値を示します。たとえば、設定可能なルール設定には、ルール合致時に実行される処理などがあります。プロファイルは、仮想 Web アプリケーション設定からのトラフィックに適用されます。

仮想 Web アプリケーション

*仮想 Web アプリケーション*は、特定のバックエンド アプリケーションのトラフィックを保護するための主要なポリシー オブジェクトです。特定のバックエンド アプリケーションのトラフィックを、メッセージ トラフィックを処理して保護するためのルール セットと処理に関連付けます。

修飾子

仮想 Web アプリケーションには修飾子を含めることができます。仮想 Web アプリケーションと同様に、修飾子はルールとセキュリティ処理を選択されたトラフィックに適用します。ただし、修飾子が選択するトラフィックは、仮想 Web アプリケーションによって処理されたトラフィックに限られます。修飾子は、仮想 Web アプリケーションによって処理されるトラフィックのサブセットにトラフィック処理設定を適用します。この設定は通常、仮想 Web アプリケーションで定義されたルールの例外を定義するのに使用されます。

Web アプリケーション セキュリティ向けのポリシー作成

Web アプリケーション セキュリティ向けのポリシー作成は通常、開発、テスト、導入を繰り返し行う反復的なプロセスとなります。一般に、効果的なポリシー作成のワークフローは次のようになります。

1. 初期プロファイルを作成します。通常、必要とされているよりも厳格なプロファイルから開始し、テスト結果に従って厳格さを緩めていく必要があります（不確かな場合は、PCI コンプライアンスのコピーから開始してください）。
2. 監視モードでプロファイルを使用する仮想 Web アプリケーションを作成します（監視モードで新しい仮想 Web アプリケーションを作成するオプションを有効に設定できます）。
3. ポリシーを導入します。
4. 予測される大容量のトラフィックを Web アプリケーションに ACE XML Gateway 経由で送信して、ポリシーをテストします。トラフィックのチェックは監視モードで行われるので、要求はブロックされません。
5. インシデント レポートをチェックして、最も多くインシデントを発生させたルールを確認します。インシデントからの false positive を識別して、必要に応じてプロファイルを修正し、不要なルールまたは署名を無効化または除外することで false positive を回避します。
6. セキュリティを維持しながら、false positive の可能性を低減させるのに必要な回数だけこのプロセスを繰り返します。

ポリシーを実稼動環境に導入した後は、インシデント レポートを監視して、false positive または悪意のあるアクティビティがないか調べることが重要です。

ルールおよび署名の拡張

Cisco ACE XML ゲートウェイ には、組み込みルールおよび署名のライブラリがあり、Web アプリケーションとそのユーザのセキュリティ保護に使用できます。組み込みルールは、クロスサイト スクリプティング攻撃、SQL および LDAP インジェクション攻撃、コマンド インジェクション攻撃など、システムに対する多くの一般的な攻撃や脅威を防止するために提供されます。また、組み込みルールや署名に、ユーザ独自のルールや署名を追加できます。ACE XML Gateway システムには、ルールと署名の記述用構文が含まれています。これによりアプリケーション固有のルールと署名を使用してシステムを拡張できます。

メッセージとハンドラの照合

着信要求は、ACE XML Gatewayのアプリケーションに定義されているユーザ インターフェイスに基づいて、指定された仮想 Web アプリケーションと照合されます。メッセージの曖昧な合致を防ぐため、Manager はユーザが同一ユーザ インターフェイスを備えた 2 つの仮想 Web アプリケーションを設定しないようにします。ただし、プレフィクス照合、正規表現、または他のユーザ インターフェイスのフィルタリング条件を使用することで、複数の仮想 Web アプリケーションを単一の要求によって照合できるポリシーの設定が可能となります。

メッセージが複数の仮想 Web アプリケーションと合致した場合、より特異性を持つユーザ インターフェイスを備えたアプリケーションが優先されます。たとえば、仮想 URL の場合は、より長いパスを持つユーザ インターフェイスが優先されることを意味します。つまり、プレフィクス照合を使用する 2 つの仮想 Web アプリケーションが次の URL を持つ場合。

- http://example.cisco.com/private
- http://example.cisco.com/

http://example.cisco.com/private/index.html は 2 番目の仮想 Web アプリケーションとも合致していますが、この URL への要求は 1 番目の仮想 Web アプリケーションによって処理されます。同一の仮想 URL を持つアプリケーションの場合、他のユーザ インターフェイス機能を使用して、次に示す特異性を決定できます。

- HTTP メソッド
- GET/POST パラメータ
- HTTP ヘッダー

これらのプロパティに基づいて特異性を決定する際、ACE XML Gatewayは次のガイドラインに従います。

1. 要求 URL とユーザ インターフェイス URL 間での完全に合致するパスは、常に最も特異性があると見なされます。
2. プレフィクスと正規表現のパスは長さで比較され、パスが長い方がより特異性があると見なされます。
3. 仮想 URL を使って決定できない場合は、パラメータと HTTP ヘッダーの合致基準を使って決定されます。より多くのパラメータまたは HTTP ヘッダー要件を定義しているユーザ インターフェイスがより特異性があると見なされます。

メッセージについて複数のハンドラの合致を特異性設定によって解決できない場合、ACE XML Gatewayは合致しているハンドラのいずれか 1 つを選択します。ただし、曖昧さの解決方法は、ポリシー設計時には予測できません。通常は、ハンドラの曖昧な合致を引き起こすポリシーを設定することは避けることが必要です。

Web アプリケーションのセキュリティ アクティビティの監視

ACE XML Gateway システムの監視ツールにより、メッセージ処理アクティビティを広範囲で確認できます。ポリシーの作成時には、監視ツールは効果的なポリシーの作成と、相互運用性問題のトラブルシューティングに役立ちます。ポリシーを実稼動環境に導入した後、監視ツールはネットワークに対する脅威を識別し、ネットワークおよびアプリケーション リソースの負荷を評価するうえで重要です。

ACE XML Gatewayでは Web アプリケーションのセキュリティ アクティビティに関する情報がいくつかの形式で表示されます。[Dashboard] ページのトラフィック モニタ グラフでは、ハンドラによるトラフィック処理レートに関するダイナミック情報が提供されます。サービス ヘルス サマリーには、Web アプリケーションのセキュリティ インシデントが高レベルで表示されます。インシデントとは、Web アプリケーション プロファイル機能（メッセージ インスペクション ルール、メッセージ リライト ルール、またはアクティブ セキュリティ機能など）が監視モードまたは有効モードのメッセージに適用されるイベントです。

ダッシュボードには、システム アクティビティとイベントの概要が表示されます。詳細は、イベント ログと Web App Firewall Incidents（Web アプリケーション ファイアウォール インシデント）レポートで確認できます。イベント ログには、すべてのシステム アクティビティに関する詳細情報が記録されます。一方、Web App Firewall Incidents（Web アプリケーション ファイアウォール インシデント）ページには、特に Cisco ACE XML ゲートウェイの Web アプリケーションのセキュリティ アクティビティに関する統計情報が表示されます。

インシデント レポートには、特定の仮想 Web アプリケーションで受信されたメッセージの数と、このアプリケーションによって適用された特定のルールがトリガーされた回数が表示されます。これにより、ACE XML Gatewayに見られる脅威の種類と、指示が行われた発信元を迅速に決定できます。

仮想 Web アプリケーションまたはルールは監視モードで動作することに注意してください。メッセージが監視モードで処理されている場合、メッセージが違反したすべてのルールが報告されます。一方、有効モードでは、メッセージはブロッキング ルールがトリガーされた最初のインスタンスで拒否されるため、プロファイルの他のルールに照らし合わせての評価は行われません。これは、イベント ログまたはインシデント レポートに表示されるのは、メッセージのブロックの原因となったルールだけで、違反の可能性があるその他のルールは処理を続行することを意味します。

（注） インシデント レポートには、最新の 24,000 イベントに関する情報だけが表示されます。この制限を超えると、最も古いイベントの情報は統計に表示されません。履歴情報のアーカイブが重要な場合は、[Web App Firewall Incidents] ページでインシデント情報をファイルに定期的にエクスポートしてください。

インシデント レポートを使用するには、操作メニューの [Web App Firewall Incidents] リンクをクリックします。このページでは、表示を次のとおり設定できます。

- [URL]：クライアントが要求する URL 別に集計された統計を表示します。
- [Virtual Web App]：ポリシー内で仮想 Web アプリケーション オブジェクト別に集計された統計を表示します。
- [Web App Group]：仮想 Web アプリケーション別に集計された統計を表示します。
- [Rule Set]：ルール グループ別に集計された統計を表示します。

これ以降ポリシーから削除された仮想 Web アプリケーションに関連するインシデントは、ルール セット別に集計された統計値だけに反映されます。表示が URL または仮想 Web アプリケーション別の場合、ポリシーから削除された仮想 Web アプリケーションのインシデントは、統計に反映されません。

表示を時間別に集計して、指定した時間範囲内に発生した統計を表示することもできます。

[Export Raw Data] ボタンを使用して、表示されている情報をエクスポートして、アーカイブや解析に使用できます。統計は、CSV 形式ファイルまたは XML 形式ファイルで書き込まれます。エクスポートされたデータには、現在ページで選択されている時間枠が反映されることに注意してください。

（注）　インシデント レポートを表示する際、サブポリシー間で移動されたハンドラは、以前のサブポリシーでのアクティビティについては、ハンドル名ではなく内部オブジェクト番号で識別されます。

基本設定のアップデート

基本設定には、Cisco ACE XML ゲートウェイで使用されている、Web アプリケーションを保護するための組み込みアーティファクトやリソース（組み込み署名、ルール、プロファイルなど）が含まれます。

シスコでは、基本設定のアップデートを発行したり、サードパーティによる基本設定のアップデートを認定する場合があります。アップデートには通常、組み込み署名、ルール、およびプロファイルの強化機能や拡張機能が含まれます。基本設定のアップデートを適用すると、システムに新しいルールや署名が導入されます。

基本設定のアップデートは、シスコが認定した基本設定ファイルを使用して実行することが必要です。この機能は、ユーザが作成したファイルのアップロードを目的としたものではありません。基本設定パッケージは、署名済みのアーカイブ ファイルで構成され、ここに新しい基本設定データが収録されています。

新しい基本設定を適用するには、[Rules & Signatures] ページで [Update Base Configuration] ボタンをクリックします。[Update Base Configuration] ページで、基本設定アップデート ファイルをロードします。

基本設定をアップデートしても、既存のポリシー設定には影響しません。つまり、組み込み署名、ルール、およびプロファイルに依存している現在の設定は、基本設定アップデートが適用された後も、変更されません。

基本設定には、YYYYMMDDXX という形式のバージョン記述子が付きます。

- YYYY は発行年です。
- MM は発行月を示し、1 桁の月には先頭にゼロが付きます。
- DD は発行日を示し、1 桁の日には先頭にゼロが付きます。
- XX は、当日中の発行回数を示す十進数の 2 桁のカウンタです。

基本設定をアップロードする場合、Manager は、ユーザがインストールしている基本設定が、すでにインストールされている基本設定の *後に* 発行されたものであることを確認します。そうでない場合、Manager はユーザに警告しますが、古い設定ファイルのロードを禁止するわけではありません。ただし、新しい基本設定を古い基本設定でアップデートすることは推奨しません。これは、新しいベース設定のルールや署名に依存する設定でコンパイル エラーが発生するおそれがあるためです。