CHAPTER 26

プロファイルに関する作業

この章では、プロファイルについて説明します。内容は次のとおりです。

プロファイルについて

プロファイルはルール グループとアクティブなセキュリティ設定のネームド コレクションで、仮想 Web アプリケーションのトラフィックの処理方法と検証方法を決定します。システムには組み込みプロファイルが含まれています。これは独自のアプリケーション特有のプロファイルで補完できます。

一般的に、Web アプリケーション セキュリティの実装では、ACE XML Gateway で処理するトラフィックの各クラスに対してプロファイルが作成されます。プロファイル設定には、特定のルールがオフまたはオンのどちらであるかと、設定可能な設定の値が含まれます。また、ルールをブロックするか処理を続行するか、ルールの一致による処理も指定します。

組み込みプロファイルはパススルー プロファイルであり、PCI 準拠プロファイルです。組み込みプロファイル設定は直接修正できません。代わりに、組み込みプロファイルの設定を修正するために、組み込みプロファイルに基づいて新しいプロファイルを作成し、新しく作成したプロファイルの設定を修正する必要があります。作成するプロファイルは仮想の Web アプリケーションで直接適用したり、同様に追加プロファイルを作成するための設定テンプレートとして使用できます。

プロファイルの設定を表示するには、操作メニューの [Profiles] リンクをクリックしてから、表示するプロファイルの名前をクリックします。組み込みプロファイルの場合、アクティブ セキュリティ機能またはルールの名前の横にある [view] リンクをクリックすると、ルール設定を表示できます。ユーザが作成したプロファイルの場合、プロファイル ページのルールの横にある [edit] リンクをクリックすると、プロファイル ルール設定を表示または修正できます。プロファイルには 3 種類のメッセージの処理および検証ルールがあります。アクティブ セキュリティ機能、メッセージ リライト ルール、およびメッセージ インスペクション ルールです。

組み込みプロファイル

組み込みプロファイルは、プリセット ルール設定を持つプロファイルです。設定は、通常、PCI 準拠要件など、要件の特定のセットを処理するためのものです。組み込みプロファイルのルール設定は直接修正できませんが、組み込みプロファイルに基づいて新しいプロファイルを作成し、必要に応じて修正できます。

組み込みプロファイルは、システムの基本設定の一部です。基本設定は更新して、追加の組み込みプロファイルを作成したり、既存の組み込みプロファイルを拡張できます。基本設定の更新には、シスコの認証が必要です。また、直接修正はできません。

デフォルトの基本設定には、これらの組み込みプロファイルが含まれます。

- パススルー プロファイル
- PCI 準拠

パススルー プロファイル

パススルー プロファイルは、すべてのルールがディセーブルになり、事実上「空白」のプロファイルになる組み込みプロファイルです。パススルー プロファイルは、初期のシステム テストを行う場合に有効です。トラフィックには決して影響しないように設定されているため、接続性やその他の初期設定のテストに使用できます。新しいプロファイルを作成する場合の基礎とすることもできます。

PCI 準拠

PCI 準拠プロファイルは、クレジットカード業界の Data Security Standard（DSS; データ セキュリティ基準）によって指定された要件を満たすために役立つ基本設定を提供します。プロファイルは、クロスサイト スクリプティング（XSS）攻撃（PCI 6.5.4）、バッファ オーバーフロー攻撃（PCI 6.5.5）、SQL インジェクションなどのインジェクション フロー（PCI 6.5.6）に対する保護に役立ちます。また、応答でクレジット カード番号のリライト ルールも指定します。このリライト ルールは、応答で顧客のクレジット カード データが誤って転送されないようにするためのものです。

プロファイルの設定の詳細については、[Profiles] ページのプロファイル名をクリックします。

（注）　組み込み PCI 準拠プロファイルは変更できませんが、このプロファイルに基づいてプロファイルを作成し、必要に応じて修正できます。

PCI 準拠の詳細については、『Cisco PCI Solution for Retail 2.0 Design and Implementation Guide』を参照してください。https://www.pcisecuritystandards.org/ も参照してください。

新しいプロファイル

カスタマイズしたプロファイル設定を定義して使用するには、新しいプロファイルを作成します。プロファイルの作成にはいくつかの手順を実行します。まず、名前や説明などが初期設定のプロファイルを作成します。その後、プロファイルのルール設定をカスタマイズし、必要なルールとセキュリティ処理をイネーブルにして、パラメータ値と重大度を設定します。

新しいプロファイルを作成するには、次の手順に従います。

ステップ 1　操作メニューで [Profiles] リンクをクリックします。

ステップ 2　[New Profile] ボタンをクリックします。

ステップ 3　次の表で説明する設定でプロファイルを設定します。

表 26-1　　プロファイルの設定

ラベル	説明
Profile Name	プロファイルを説明する一意の名前。この名前は、ポリシー内のプロファイルを識別するために使用します。
Description	プロファイルのオプションの説明。この値は、他の Web コンソールのユーザに Web コンソール内のプロファイルを説明するために役立ちます。説明の値がコンソールの外に表示されることはありません。
Copy Settings From	既存のプロファイルの初期ルールとアクティブ セキュリティ設定として使用します。ソース プロファイルの設定は、プロファイルの作成時にしか新しいプロファイルに反映されないことに注意してください。つまり、ソースとして使用されたプロファイルへのその後の変更は、そのソースから生成したプロファイルに自動的に反映されません。 設定済みの設定なしにプロファイルを作成するには、デフォルトの選択肢である none を維持します。

ステップ 4　[Create Profile] ボタンをクリックします。

指定した設定に基づいて新しいプロファイルが作成され、その設定ページが表示されます。

ステップ 5　プロファイル設定ページから、必要に応じてプロファイルのルールとアクティブ セキュリティ機能を修正します。ルールの横にある [edit] リンクをクリックしてイネーブルにするか、このプロファイルのコンテキストで再設定します。

プロファイルでアクティブ セキュリティ、インスペクション ルール、リライト ルールを設定した後、仮想 Web アプリケーションでプロファイルを適用できます。

アクティブ セキュリティ機能

プロファイル内のアクティブ セキュリティ機能は、データ オーバーフロー ディフェンス、HTTP ヘッダー処理、クッキー暗号化/復号化など、特別なメッセージ処理やセキュリティ タスクを実行します。

（注）　ルールや署名とは異なり、アクティブ セキュリティ機能はシステムに追加できません、または設定で提供されている場合を除きカスタマイズできません。

一般に、モニタ モードの仮想 Web アプリケーションでは、ACE XML Gateway はセキュリティ ルールをトラフィックに適用しますが、ルールに違反したメッセージをブロックすることはありません。アクティブ セキュリティ機能のほとんどは、HTTP ヘッダー処理、HTTP 例外マッピング、クッキー セキュリティなど、モニタ モードの仮想 Web アプリケーションにも影響し続けます。しかし、データ オーバーフロー ディフェンスと Referer 適用はモニタ モードになります。つまり、起動すると、イベントは記録されてもメッセージはブロックされません。

一般的に、プロファイルのアクティブ セキュリティ設定を表示または修正するには、操作メニューの [Profiles] リンクをクリックしてから、表示するプロファイルの名前をクリックします。アクティブ セキュリティ機能名の横にある [view] リンク（組み込みプロファイルの場合）または [edit] リンク（ユーザが作成したプロファイルの場合）をクリックして設定にアクセスします。

以降のセクションでは、各セキュリティ機能について詳しく説明しています。

HTTP ヘッダー処理

逆プロキシとして、ACE XML Gateway はメッセージ内の特定の HTTP ヘッダーを自動的に処理して入力します。たとえば、メッセージの処理時に `Date` および `Content-Length` ヘッダーに適切な値を入力します。しかし、メッセージ内のその他のタイプの HTTP ヘッダーは修正されずにパススルーされます。ACE XML Gateway では、ヘッダーをパススルーせずに、メッセージ内の特定のヘッダーを修正、追加、または削除できます。

HTTP ヘッダー処理ページは、`Server` ヘッダーや `X-Forwarded-For` ヘッダーなど、しばしば逆プロキシで操作する必要のある HTTP ヘッダーの設定を制御します。さらに、名前によって識別される HTTP ヘッダーの特別な処理を設定できます。HTTP ヘッダー処理は要求または応答サイドで指定できます。

特定タイプのヘッダーの値は、ポリシーで設定できません。一般に、これらのヘッダーには `Date` ヘッダーや `Content-Length` ヘッダーなど、ランタイムに決定される値が入力されます。さらにヘッダーパススルーは「ホップバイホップ」ヘッダーと見なされるものには適用されません。これは次のような単一の転送レベル接続のコンテキストでは重要です。

- 受け入れエンコード
- 接続
- キープアライブ
- プロキシ認証
- プロキシ許可
- TE
- トレーラ
- 転送エンコード
- アップグレード

次の表は、HTTP ヘッダー処理設定について説明しています。

表 26-2　HTTP ヘッダー処理設定

ラベル	説明
Insert "X-Forwarded-For" header with client's IP address	逆プロキシ サーバはしばしば X-Forwarded-For HTTP ヘッダーを使用して要求をバックエンド システムに送信したクライアントを特定します。このヘッダーを使用して、ACE XML Gateway から受信された要求ソースとして表示される IP アドレスをバックエンド アプリケーションに示せます。ヘッダーはこれらのオプションの 1 つによって指定されたとおりに追加されます。 • [if the header does not already exist]：メッセージに表示されない場合に限りヘッダーを追加します。ヘッダーがすでに存在する場合、ヘッダーは元の値でパス スルーされます。 • [replacing any existing value]：既存のヘッダーを削除して、カスタム ヘッダーを追加します。 • [in addition to any existing value]：メッセージ既存であるかに関係なくヘッダーを追加します。この名前のヘッダーがメッセージにすでに存在する場合、ヘッダーの 2 つのインスタンスになります。 • [appending to any existing value]：ヘッダーがすでに存在する場合、カンマとソースの IP アドレスを既存のヘッダーに追加します。メッセージにヘッダーがない場合、追加されます（特に広く使用されている Squid オープン ソース Web プロキシの場合、最上の相互運用性のためにこのオプションを推奨します）。
Insert Client SSL Certificate DN in header named	新しいヘッダーとして、メッセージに含まれるクライアント SSL 認証のサブジェクトの認定者名を挿入します。DN 値はヘッダーに指定した名前で追加されます。ヘッダーはこれらのオプションによって指定されたとおりに追加されます。 • [if the header does not already exist]：メッセージに表示されない場合に限りヘッダーを追加します。ヘッダーがすでに存在する場合、ヘッダーは元の値でパス スルーされます。 • [replacing any existing value]：既存のヘッダーを削除して、カスタム ヘッダーを追加します。 • [in addition to any existing value]：メッセージ既存であるかに関係なくヘッダーを追加します。存在する場合、このヘッダーの 2 つのインスタンスになります。 • [appending to any existing value]：ヘッダーがすでに存在する場合、カンマと証明書 DN を既存のヘッダーに追加します。メッセージにヘッダーがない場合、追加されます。 このオプションによってヘッダーに追加する証明書 DN 値の場合、[I/O Process Settings] ページに指定したように、SSLVerifyClient 設定は optional_no_ca 値に設定する必要があります。そうでない場合、ヘッダーには空白の値が追加されます。
Rewrite "Host" header with destination server hostname	選択された場合、仮想 Web アプリケーション定義に指定した宛先サーバから派生したとおり、要求の Host ヘッダー値を宛先バックエンド ホストの名前で置き換えます。

ラベル	説明
Custom Header Processing	要求メッセージの場合、ネームド HTTP ヘッダーで次の処理を行います。これらの値を指定してヘッダー処理を設定します。 • 最初のフィールドで処理するヘッダーの名前を入力します。 • 操作メニューでヘッダーの処理方法を指定します。 – [strip]：指定したネームド ヘッダーのすべてのインスタンスをメッセージから削除します。これはヘッダーが予想されることを意味するものではありません。つまり、ヘッダーがなくてもエラーではありません。 – [set if empty]：ネームド ヘッダーが存在しない場合、指定した値で挿入します。存在する場合は、何も実行されません。生成されるメッセージには、設定した名前の少なくとも 1 つのヘッダーが含まれます。 – [replace value]：ネームド ヘッダーの既存のオカレンスを削除し、指定した値の新しいインスタンスを挿入します。 – [add value]：指定した名前と値のヘッダーの新しいインスタンスを挿入します。このオプションは同じ名前の既存のヘッダーには影響しません。そのため、少なくとも 1 つ、場合によっては同じ名前の複数のヘッダーを持つメッセージとなります。 – [append]：同じ名前の既存のヘッダーにカンマに続いて設定値を付加します。要求にネームド ヘッダーがない場合、追加されます。同じ名前の複数のヘッダーがある場合、値はヘッダーの 1 つだけに付加されます。 動作は、インターフェイスに表示される順序で実行されます。 • （[strip] オプションを選択していない限り）動作後にテキスト フィールドに目的の値を入力します。このフィールドは、Reactor 表現の形式でダイナミック値をサポートします（例：$(REQUEST_HEADER['Date'])） Reactor 表現構文の詳細については、『*Cisco ACE XML Gateway User Guide*』を参照してください。
Replace "Server" header value with	デフォルトでは、仮想 Web アプリケーションによって処理される応答で、バックエンド システムから受信された Server ヘッダー値は発信応答にパス スルーされます。 または、ACE XML Gateway で `Server` ヘッダーをこのフィールドで指定された値にリライトできます。

ラベル	説明
Custom Header Processing	応答メッセージの場合、ネームド HTTP ヘッダーで次の処理を行います。これらの値を指定してヘッダー処理を設定します。 • 最初のフィールドで処理するヘッダーの名前を入力します。 • 操作メニューでヘッダーの処理方法を指定します。 – [strip]：指定したネームド ヘッダーのすべてのインスタンスをメッセージから削除します。これはヘッダーが予想されることを意味するものではありません。つまり、ヘッダーがなくてもエラーではありません。 – [set if empty]：ネームド ヘッダーが存在しない場合、指定した値で挿入します。存在する場合は、何も実行されません。生成されるメッセージには、設定した名前の少なくとも 1 つのヘッダーが含まれます。 – [replace value]：ネームド ヘッダーの既存のオカレンスを削除し、指定した値の新しいインスタンスを挿入します。 – [add value]：指定した名前と値のヘッダーの新しいインスタンスを挿入します。これは同じヘッダー名の既存のオカレンスに影響しません。このため、少なくとも 1 つ、場合によっては同じ名前の複数のヘッダーを持つメッセージとなる場合があります。 – [append]：同じ名前の既存のヘッダーにカンマに続いて設定値を付加します。応答にネームド ヘッダーがない場合、追加されます。同じ名前の複数のヘッダーがある場合、値はヘッダーの 1 つだけに付加されます。 動作は、インターフェイスに表示される順序で実行されます。 • （[strip] オプションを選択していない限り）動作後にテキスト フィールドに目的のヘッダー値を入力します。

HTTP 例外マッピング

HTTP 例外は、要求の処理中にエラーまたはその他の予期せぬイベントを警告する応答メッセージです。例外は、要求自体のエラーから発生する場合や、バックエンド システム処理またはネットワークのエラーから発生する場合があります。場合によって、バックエンド アプリケーションから渡された HTTP 例外には、Web サーバ スタック トレースなど、ハッカーが使用できる、潜在的な攻撃者への機密情報が含まれる可能性があります。Cisco ACE XML ゲートウェイ での例外のマッピングにより、一般的なエラー メッセージだけがクライアントに渡されるようにできます。

例外マッピングがイネーブルの場合、特定のエラー情報を返す代わりに、ACE XML Gateway は設定した応答を返します。たとえば、400 および 500 のエラーすべてを一般的な 500 のエラーにマッピングするよう設定したり、いくつかのエラーに特定の応答を設定できます。

次の表は、HTTP 例外処理設定について説明しています。

表 26-3　HTTP 例外処理設定

ラベル	説明
For server errors (status code 400 and above) not specified below	このオプションを使用して、400 以上の HTTP ステータス コードを持つバックエンド システムからのエラー応答をクライアントに返される一般的なエラー応答にマッピングします。デフォルトで、このような応答はクライアントにパス スルーされます。 一般的な HTTP 500 ステータス コード応答は次の説明でサーバ エラーを報告します。"The server encountered an internal error and was unable to complete your request" このエラー マッピング オプションはその下のカスタム応答マッピング オプションとともにイネーブルにできます。カスタム応答設定は、どちらも適用できるエラー コードを持つ応答に対するこの一般的なマッピングより優先されます。 このオプションがパススルーに設定され、例外に特定のステータス コードがマッピングされている場合、クライアントから受信したエラー応答の `Server` ヘッダー値は変化します。パススルーした値は、バックエンド システムによって設定された `Server` 値となり、マッピングされたエラーは、ポリシー設定で指定されている場合、ACE XML Gateway で設定された `Server` 値となります。
Status Codes	エラー応答をすべて一般的な応答にマッピングするのではなく、バックエンド システムから受信した特定の HTTP エラー コードにカスタム応答メッセージを設定できます。 この動作を設定するには、[Status Codes] フィールドで、カスタム応答にマッピングする応答の数字のエラー ステータス コードを入力します。数字を個別に、または "400, 403, 500-599" のように範囲で入力できます。範囲と単一の値はカンマで区切る必要があります。 導入されると、指定したエラー コードを持つバックエンド ネットワークからの応答は、クライアントへの配信のために設定した応答にマッピングされます。この設定は、一般的なマッピング設定よりも優先されます（設定されている場合）。
Status Code	発信応答メッセージのステータス コード。着信応答からのステータス コードのパス スルーまたはプリセット ステータス コードの使用のオプションを備えています。
Content-Type	発信応答メッセージのコンテンツ エンコード タイプ。デフォルトではテキスト /html です。
Other Headers	応答に含めるその他の HTTP ヘッダー。 このフィールドで特定の HTTP ヘッダーを指定することはできないことに注意してください。たとえば、Date および Content-Length ヘッダー値は、バックエンド応答からパス スルーされ、ここで手動で特定はできません。また、Server ヘッダー値はバックエンド システムからパス スルーされるか（デフォルト）、HTTP ヘッダー処理設定でより具体的な設定が読み込まれます。
Response Body	クライアントに送信される HTTP 応答の本文。

リファラーの適用

referrer HTTP 要求ヘッダー（または標準で間違ってつづられた `Referer`）は、要求が Request-URI を取得したリソースのアドレスを示します。リファラーの適用機能は、Cross Site Request Forgery（CSRF）と呼ばれる種類の攻撃に対して保護を行えます。

CSRF 攻撃の一般的な例では、オンラインのバンキング アプリケーションなど、機密情報のある Web アプリケーションとアクティブなブラウザ セッションを行っているユーザが対象となります。認証されたセッションがアクティブな間に、攻撃者の口座への送金などの動作をバンク アプリケーションに対して開始させる別の Web サイトのリンクをクリックするようユーザが促された場合、その動作が実行される可能性があります。リンクは、電子メールやパブリック フォーラムなどで、攻撃者によって管理されている Web サイト上に提示されます。

このような攻撃は `Referer` ヘッダーで示されたホストに基づいてメッセージを制限すると避けることができます。リファラー値に指定されたホストが Web アプリケーション自体のホストではない場合、要求は拒否される可能性があります。これは、機密操作を実行する要求 URL がサードパーティの Web サイト上のリンクや電子メールからなど、別の場所で取得された要求をブロックします。

次の表はリファラーの適用設定について説明しています。

表 26-4　　リファラーの適用設定

ラベル	説明
If the "Referer" header is present, require that its value matches requested host name	選択されている場合、`Referer` ヘッダーを含む要求はその値として、要求 URL の 1 つに一致するホスト名を持つ URI を持っている必要があります。つまり、リファラーは、外部アプリケーションや Web サイトではなく、要求によって処理された Web アプリケーションを特定する必要があります。
Never check "Referer" header on GET requests	HTTP GET 要求は通常、このタイプの攻撃では使用されないため、GET 要求のチェックをディセーブルにできます。チェックは POST 要求またはその他の HTTP メソッドを備えた受信メッセージに適用されます。
Monitor Mode	選択した場合、`Referer` ヘッダーで特定したホストが要求 URL に一致しないと、イベントが記録されますが、メッセージは許可されます。

HTTP クッキー セキュリティ

Web アプリケーションは HTTP クッキーを使用して特定のユーザやセッションに関する情報を保存する場合があります。サーバはクライアントに送信される応答にクッキーを組み込み、ブラウザはその後の要求でクッキーをそのまま返します。クッキーはプライベート情報を格納したり、セッション ハイジャック攻撃の基盤を形成することができます。ほとんどの場合、クッキーのコンテンツはバックエンド アプリケーションから以外、修正しないでください。

クッキー セキュリティがイネーブルかどうかに関係なく、メッセージ内のクッキーはデータ オーバーフローとプロファイルで設定した HTTP ヘッダー処理設定の対象となります。クッキー セキュリティをイネーブルにして、ACE XML Gateway はクッキー特有の検証方法を適用し、クライアントに配信する前にクッキーを暗号化または署名してクッキーのセキュリティを確保できます。

クッキーを処理した後、クライアントからのその後の要求で ACE XML Gateway がクッキーを受信すると、バックエンド Web アプリケーションに転送する前に署名をチェックするか、クッキーを復号化します。ACE XML Gateway は、それによってクッキーが修正されていないことや Gateway からクライアントに表示されていないことを確認できます。

クッキー セキュリティがイネーブルの場合、ACE XML Gateway は署名の確認、クッキーの復号化、またはクッキーの正確さの検証ができないことに基づいて、無効とわかったクッキーを削除します（クッキー セキュリティがディセーブルの場合、クッキーは ACE XML Gateway にそのまま反映されます）。値に閉じていない引用符、重複したアトリビュート、および特定の禁止された文字（カンマ（,）、セミコロン（;）、二重引用符（"）、等記号（=）、空白など）が含まれている場合、クッキーは無効と見なされます。

（注） クッキー セキュリティは、Javascript を使用してクライアントでクッキーを設定または修正するアプリケーションには使用しないでください。たとえば、クライアント側の Javascript はバックエンド アプリケーションにブラウザ タイプを示すためにクッキーを設定する場合があります。クライアントが修正したクッキーは検証や復号化に失敗するため、このような場合はクッキー セキュリティはディセーブルにする必要があります。クッキー署名をイネーブルにすると、クライアントで追加された新しいクッキーが Gateway によってドロップされることに注意してください。ただし、暗号化をイネーブルにすると、新しいクッキーは受け入れられます。どちらの場合も、クライアントで修正されたクッキーはドロップされます。

クッキー セキュリティがクッキーの暗号化や署名の使用によって明示的にイネーブルにされると、クッキー ヘッダーの検証が行われます。次の表は、アクティブなクッキー セキュリティ機能の設定について説明しています。

表 26-5　クッキー セキュリティ機能

ラベル	説明
Sign (HMAC-SHA1)	クライアントに送信し、後続の要求で返された際に検証する前に、デジタル署名された応答にクッキーを格納するためにこのオプションを選択します。デジタル署名はクッキーの完全性を確保するために役立ちます。これは、（たとえば、セッションのスプーフィングなどの目的で）悪意を持って改ざんされたクッキーが保護されたアプリケーションに転送されるのを防ぐことができます。クッキー署名が無効な場合、クッキーは要求から削除されます。 Cisco ACE XML ゲートウェイ は、ポリシー設定のパスフレーズ フィールドに指定する秘密鍵に基づいて、入力された Hash Message Authentication Code（HMAC または KHMAC; ハッシュ メッセージ認証コード）を使用してクッキーを署名します。別の ACE XML Gateway クラスタによって処理されたクッキーを持つ要求を受信する ACE XML Gateway クラスタは、同じ署名パスフレーズを使用する必要があります。 このプロファイルでデータ オーバーフロー ディフェンスも使用している場合、クッキー署名の影響を考慮する必要があります。クッキーを署名すると、Cisco ACE XML ゲートウェイ は発信メッセージにさらにヘッダー（署名クッキー）を追加します。署名は常に 8 文字の長さで、クッキー ヘッダーの名前は 3 文字長くなります。このため、署名クッキー ヘッダーの合計サイズは、元のクッキー値アトリビュートが 10 文字以下の場合、元のクッキーのサイズより大きくなります。たとえば、次のクッキーを使用するとします。 Cookie: NAME=123456789a 署名すると、メッセージには次の形式で（実際の署名ではなく）署名クッキーが含まれます。 Cookie: NAMESig=12345678 このように、クッキー値は常に 8 文字で表されます。ただし、名前にはさらに 3 文字が追加されます。

ラベル	説明
Encrypt (AES)	クライアントに配信する前に Cisco ACE XML ゲートウェイ でメッセージ内のクッキーを暗号化するためにこのオプションを選択します。その後の要求でクライアントから暗号化されたクッキーを受信すると、バックエンド アプリケーションに配信する前にクッキーを復号化します。 クッキーの暗号化は、クライアントからクッキー データを隠すために機能します。クッキーはサーバと同様にクライアントによって生成できることに注意してください。（クライアントが生成したクッキーを示す）非暗号化クッキーを持つ要求を受信すると、ACE XML Gateway はこの通過を許可します。このため、一般的な暗号化が完全性の保護を行える一方、この場合、ACE XML Gateway はすべてのクッキーの暗号化を必要としないため、クッキーの完全性を確保するために暗号化に依存できないことに注意することが重要です。 Cisco ACE XML ゲートウェイ は対称キーベースの暗号化標準である Advanced Encryption Standard（AES; 高度暗号化規格）を使用してクッキーを暗号化します。暗号テキストはパスフレーズ フィールドで指定した秘密鍵によって生成されます。 クッキー ヘッダーのサイズに制限を課す可能性のあるデータ オーバーフロー ディフェンスも使用している場合は、クッキー暗号化の影響を考慮する必要があります。暗号化の場合、クッキーは元のクッキー値のサイズに比例したバイト数だけ大きくなります。特に、暗号化されたクッキーの長さは次の公式を使用して予想できます。これらは個別に暗号化されるため、各クッキーの名前と値の長さを使用して、それを次の 16 の倍数に繰り上げます。その後、3 で割り(余りがある場合繰り上げ)、4 を掛けます。 たとえば、名前が 10 文字の場合、10 + 1 = 11 となり、16 に繰り上げ、3 で割って 6 に繰り上げて 4 を掛け、24 になります。一部の名前 / 値の長さの例と暗号化後のサイズは次のようになります。 • 0 ～ 15 は 24 文字になります。 • 16 ～ 31 は 44 文字になります。 • 32 ～ 47 は 64 文字になります。 この計算の結果を使用して、使用する適切なデータ オーバーフロー設定を決定します。
Cookies with Passphrase	クッキーを暗号化または署名するための秘密鍵。入力したパスフレーズは少なくとも 5 文字の長さである必要があり、数字、文字、または特殊文字を組み合わせて使用できます。 パスフレーズの長さは 5 文字でもかまいませんが、セキュリティを強化するためにはもっと長いパスフレーズを入力する必要があります。理想的には、20 文字程度の長さにしてください。 ポリシーが導入されると、Manager がパスフレーズをクラスタ内のすべての Cisco ACE XML ゲートウェイ に転送します。個別に管理されているクラスタが後続の要求を同じクライアントから受信する場合、これらのクラスタは同じパスフレーズで設定されている必要があります。

データ オーバーフロー ディフェンス

データ オーバーフロー ディフェンスでは、メッセージ内のさまざまなアトリビュートのサイズと数に基づいてセキュリティを設定できます。データ オーバーフロー ディフェンス設定に適合しないメッセージはブロックされたり、設定可能な重大度で記録されたイベントでパス スルーされる可能性があります。

（注）　仮想 Web アプリケーション自体の処理設定はメッセージ構成要素のサイズに影響する可能性があります。たとえば、クッキーの署名や暗号化は新しいヘッダーを導入したり、既存のヘッダーを拡大する可能性があります。データ オーバーフロー ディフェンスは、クッキーの処理後にメッセージに適用されます。詳細については、「HTTP クッキー セキュリティ」（P.26-259）を参照してください。

次の表は、データ オーバーフロー ディフェンス設定について説明しています。

表 26-6　データ オーバーフロー ディフェンス設定

ラベル	説明
Enforce the following data limits on requests	データ オーバーフロー保護をイネーブルにして、データ オーバーフロー ディフェンスの設定を使用可能にする場合にこのオプションを選択します。
Maximum Number of HTTP Headers	メッセージで許可される HTTP ヘッダーの数。
Maximum Size of Any HTTP Header	HTTP ヘッダーのバイト単位の最大サイズ。これはクッキーには適用されません。
Maximum Cookie Size	HTTP クッキーまたは暗号化されたクッキー ヘッダーのバイト単位の最大サイズ。
Maximum Total HTTP Header Size	クッキーを含む KB 単位の HTTP ヘッダーすべての最大合計サイズ。
Maximum Size of Request URL	要求 URL のバイト単位の最大サイズ。この値には、要求されたホスト名、リソース、すべての URL パラメータが含まれます。
Maximum Size of GET Query String	URL 内の GET クエリー ストリングのバイト単位の最大サイズ。クエリー ストリングは、http://hostname/path/page?query_string のように、要求の疑問符の後に表示されます。
Maximum Number of Request Arguments	GET または POST 要求の引数の最大数。GET 要求では、引数は http://example.com/path/page?name1=value1&name2=value2 のように URL にアンパサンドで区切られたパラメータとして表示されます。 POST 要求では、要求の本文で同様の名前と値のペアとして表示されます。
Maximum Size of Any Argument	引数の名前と値のバイト単位のサイズを含む、POST または GET 要求の引数の 1 つの最大サイズ。
Maximum Total Size of Request Body	要求の POST 本文のバイト単位の最大合計サイズ。
Monitor mode	選択すると、データ オーバーフロー設定に違反する要求は、設定された重大度で記録されるイベントとなりますが、ブロックはされません。

ラベル	説明
Event Log	ルール グループ レベルまたは仮想 Web アプリケーション レベルでモニタ モードで適用された場合、この処理の起動によるログ イベントの重大度を制御します。 デフォルトで、これらのイベントは警告レベルで記録されます。しかし、ルールがモニタ モードで適用された場合、重大度を下げた方が適当な場合もあります。
Response	メッセージがデータ オーバーフロー ディフェンス設定に違反した場合に ACE XML Gateway が実行する必要のある処理。オプションは次のとおりです。 • ステータス コード 400、クライアント エラーで HTTP エラー応答を返します。 • ステータス コード 500、サーバ エラーで HTTP エラー応答を返します。 • 設定したカスタム HTTP エラー応答を返します。 • 許可メッセージはモニタ モードと同様です。署名一致イベントは報告されますが、メッセージはパススルーを許可されます。

メッセージ リライト ルール

メッセージ インスペクション ルールはブロックまたは許可することによりメッセージ全体で動作しますが、リライト ルールはパス スルーする前に一致したコンテンツを置き換えてメッセージを修正します。また、メッセージ インスペクション ルールが要求で動作するのに対し、メッセージ リライト ルールは応答で動作します。

メッセージ リライト ルールは、ユーザのクレジット カード番号や社会保障番号などのような機密情報をバックエンド アプリケーションが送信しないように支援します。リライト ルールの署名に一致する応答の部分は、置換文字に置き換えられます。メッセージ リライト ルールは、応答の署名パターンの複数のインスタンスに一致する可能性があります。

ポリシーでイネーブルになると、仮想 Web アプリケーションがモニタ モードだけに設定されている場合でも、メッセージ リライト ルールはメッセージを修正します。つまり、メッセージのリライトは、仮想 Web アプリケーションがモニタ モードでもイネーブル モードでも実行されます。

コンテンツのリライトと応答の圧縮

圧縮される可能性のある応答のコンテンツ置換を設定する場合、特別な考慮事項があります。バックエンド システムによって圧縮された応答を受信すると、Cisco ACE XML ゲートウェイ は応答をパススルーできます。しかし、メッセージ リライト ルールは圧縮された応答では機能しません。

コンテンツ置換がシステムにとって重要で、かつバックエンド システムが応答の圧縮を行う場合は、発信要求からの圧縮した応答（ACCEPT-ENCODING）の受け入れを示すために使用される HTTP ヘッダーを削除して、Gateway が圧縮されていない応答を確実に受信できるようにする必要があります。

ACCEPT-ENCODING ヘッダーが発信要求から削除される HTTP ヘッダー処理を設定して、仮想 Web アプリケーションでヘッダーの削除を指定できます。その結果、バックエンド サーバからの応答は圧縮されません。

リライト ルールをイネーブルにして設定するには、プロファイルのリライト ルール グループの横の [edit] リンクをクリックします。リライト ルールには次の設定があります。

表 26-7　リライト ルールの設定

ラベル	説明
Rule Set Mode	このプロファイルを使用する仮想 Web アプリケーションで、ルール グループをイネーブルにするかどうか。このオプションをイネーブルにすると、このルール グループのルールが表示されます。これは個別にイネーブルまたはディセーブルにできます。 オプションは次のとおりです。 • Enabled：このルール グループのルールは、このプロファイルを使用する仮想 Web アプリケーションのメッセージ トラフィックに適用されます。 • Disabled：ルールは、このプロファイルのトラフィックに適用されません。 イネーブルのリライト ルールは、仮想 Web アプリケーションがモニタ モードでも適用されることに注意してください。
view rule set details	現在のルール グループのソース コードを表示します。
Rewrite Rules	グループ内の各リライト ルールは個別にイネーブルまたはディセーブルにできます。イネーブルの場合、ルールはメッセージ トラフィックに適用されます。ルールが署名の一致によって起動されると、一致したテキストの各文字がルールの置換文字によって置き換えられます。文字はルールの [Rewrite Char.] カラムで示されます。これは、[view rule set details] リンクをクリックすると表示できます。

メッセージ インスペクション ルール

メッセージ インスペクション ルールは、要求の潜在的に悪意のあるコンテンツを調べます。ルールは、署名を使用して Web アプリケーションに誘導されるメッセージ内の対象コンテンツを特定します。組み込みメッセージ インスペクション ルールは、たとえば、コマンド インジェクションやクロス サイト スクリプティング攻撃を検出するためのものです。コンテンツが検出されると、ACE XML Gateway は要求をブロックしたり、イベントを記録してパス スルーできます。

メッセージ インスペクション ルール セットの場合、プロファイルで適用される厳密レベル（基本、中程度、または厳密）を指定できます。重大度は、セット内でイネーブルになるルールを制御します。同じまたはそれ以下の重大度のルールだけがイネーブルになります。たとえば、中程度の重大度を選択すると、ルール セット内の中程度と基本のルールがイネーブルになります。特定レベルの代わりに、カスタム オプションでイネーブルにするルールを手動で選択することもできます。

リライト ルールをイネーブルにして設定するには、プロファイルのメッセージ インスペクション ルール グループの横の [edit] リンクをクリックします。インスペクション ルールには次の設定があります。

表 26-8　インスペクション ルールの設定

ラベル	説明
Rule Set Mode	このプロファイルを使用する仮想 Web アプリケーションで、ルール グループをイネーブルにするかどうか。このオプションをイネーブルにすると、特定の重大度のこのルール グループのルールが表示されます。 オプションは次のとおりです。 • Enabled：このルール グループのルールは、このプロファイルを使用するアプリケーションのメッセージ トラフィックに適用されます。 • Monitor：メッセージがイネーブルのルールを起動すると、ルール設定（デフォルトでは警告）で指定した重大度でイベントが記録されますが、メッセージはブロックされません。 • Disabled：このルール グループのルールは、このプロファイルのトラフィックに適用されません。
Level	適用するグループ内のルールの重大度。各ルールは重大度で説明されます。重大度は、通常、数字およびルール内の署名のスコープまたは調査するメッセージのスコープで区別されます。グループの重大度を選択すると、ACE XML Gateway は同じ重大度のグループ内のルールだけを適用します。 重大度は下から基本、中程度、厳密です。イネーブルにするルールを直接選択するには、[Custom] を選択します。
Exemptions	除外では、ルールの適用方法を微調整できます。除外は、評価から特定の署名を外します。メッセージが除外署名に一致した場合、一致は無視されます。たとえば、ユーザ名を示すパラメータ内の一重引用符（'）を探す署名は、パラメータに /path?lastname=o'neill という正規の値が含まれている場合があるため、除外するのが適当な場合があります。 これらの場合、一重引用符パターン署名から lastname パラメータを除外できます。カスタム署名でも同じ効果を実現できますが、除外機能を使用した方が設定が簡単です。 除外は、ここで実行したように、基本プロファイル（ほとんどの場合に最適です）または仮想 Web アプリケーションの修飾子のプロファイルで指定できます。 除外設定で、要求全体、パラメータ、または HTTP ヘッダーのどれに適用するか除外のスコープを示します。また、特定の署名またはすべての署名が除外されるかどうかを示します。 ネームド署名の場合、次のような署名識別名で署名を示します。 **In parameter**: lastname **ignore signature**: CrossScriptXSS.52 ポリシー内の署名の署名識別名を取得するには、[Rules & Signatures] ページで [View Signatures] をクリックします。 除外がメッセージに適用されると、次の項目が情報レベルで記録されます。CROSSITESCRIPT.CrosSiteScript1:CrossScriptXSS.52:REQUEST_GETPARAM['firstname'] detected by a Limit, but an override deactivated it.

ラベル	説明
Event Log	ルール グループ レベルまたは仮想 Web アプリケーション レベルでモニタ モードで適用された場合、このルールの起動によるログ イベントの重大度を指定します。 デフォルトで、これらのイベントは警告レベルで記録されます。しかし、ルールがモニタ モードで適用された場合、ルールの重大度を下げた方が適当な場合もあります。
Response	ルール署名が一致した場合にクライアントに返される応答メッセージの設定に使用します。オプションは次のとおりです。 • ステータス コード 400、クライアント エラーで HTTP エラー応答を返します。 • ステータス コード 500、サーバ エラーで HTTP エラー応答を返します。 • 設定したカスタム エラー応答を返します。 • 許可メッセージはモニタ モードと同様です。署名一致イベントは報告されますが、メッセージはパススルーを許可されます。