CHAPTER 5

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

プロファイルとは、ルールとアクティブなセキュリティ設定の指定の集合であり、仮想 Web アプリケーションのためにトラフィックの処理方法および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あります。このプロファイルを使用して、独自の、アプリケーション固有のプロファイルを補完できます。

一般的に、Web アプリケーション セキュリティの導入には、ACE Web Application Firewall で処理されるトラフィックの各クラスのプロファイル作成が含まれます。このプロファイル設定には、指定のルールがオフかオンか、またはその設定可能な設定の値が含まれます。また、ルール照合の結果生じる動作、つまりルールを遮断するか、処理を続行するかも指定します。

組み込みプロファイルは、パススルー プロファイルおよび PCI 準拠プロファイルです。組み込みプロファイルの設定は、直接変更できません。その代わり、組み込みプロファイルの設定を変更するには、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、新たに作成したプロファイルの設定を変更する必要があります。作成したプロファイルは、仮想 Web アプリケーションに直接適用できます。または、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同様に機能できます。

プロファイルの設定を表示するには、操作メニューで [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の [view] リンクをクリックしてルール設定を表示できます。ユーザ作成のプロファイルの場合、このプロファイルのページでルールの横の [edit] リンクをクリックしてプロファイルのルール設定を表示または変更できます。プロファイルには、アクティブなセキュリティ機能、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 ルールという 3 種類のメッセージ処理および検証ルールがあります。

組み込みプロファイル

組み込みプロファイルとは、プリセットのルール設定を持つプロファイルです。この設定は、通常、PCI 準拠要件など特定の一連の要件に対応することを目的としています。組み込みプロファイルのルール設定は直接変更できませんが、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できます。このプロファイルは、必要に応じて変更できます。

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。この基本設定は更新できます。その結果、組み込みプロファイルの追加または既存の組み込みプロファイルの強化が行われます。基本設定の更新は、シスコ認定の更新である必要があります。直接変更できません。

デフォルトの基本設定には、次の組み込みプロファイルが含まれています。

- 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、すべてのルールが無効になっている組み込みプロファイルであり、事実上「空白」のプロファイルになっています。パススルー プロファイルは、システムの初期テストを行う際に役立ちます。トラフィックには決して影響を与えないように設計されているので、接続または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ための基盤としても機能します。

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）によって指定される要件要素を満たすことを目的としています。このプロファイルは、Cross-Site Scripting（XSS; クロスサイト スクリプティング）攻撃（PCI 6.5.4）、バッファ オーバーフロー攻撃（PCI 6.5.5）、および 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）に対する保護を支援します。応答に関するクレジット カード番号リライト ルールも指定します。このリライト ルールは、顧客のクレジット カード データが気付かないうちに応答に含まれて転送されないようにすることを目的としています。

プロファイル設定に関する詳細については、プロファイルのページでプロファイル名をクリックしてください。

（注）　組み込みの 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できます。このプロファイルは、必要に応じて変更できます。

PCI 準拠に関する詳細については、『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

各ユーザに合っ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、複数の手順が含まれます。まず、名前、説明などの初期設定を行ってプロファイルを作成します。次にプロファイルのルール設定をカスタマイズできます。使用するルールおよびセキュリティ動作を有効にし、パラメータ値および重大度レベルを設定します。

新しいプロファイルを作成するには、次の手順を実行します。

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　次の表に記載された設定を使用してプロファイルを設定します。

表 5-1　　プロファイル設定

ラベル	説明
[Profile Name]	プロファイルの一意の記述名。この名前は、ポリシーでプロファイルを識別するのに使用されます。
[Description]	プロファイルの説明（任意）。この値は、他の Web コンソール ユーザに対して Web コンソール内のプロファイルを記録するのに役立ちます。この説明の値は、コンソール外には表示されません。
[Copy Settings From]	このプロファイルの初期ルールおよびアクティブなセキュリティ設定として既存のプロファイルのルールやセキュリティ設定を使用します。ソース プロファイルの設定は、プロファイルの作成時にだけ新しいプロファイルに反映されます。つまり、ソースとして使用されるプロファイルに対するそれ以降の変更が、そこから生成されたプロファイルに自動的に反映されることはありません。 事前設定を使用せず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] のままにします。

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　プロファイルの設定ページで、プロファイルの必要に応じてルールおよびアクティブなセキュリティ機能を変更します。ルールの横の [edit] リンクをクリックして、ルールを有効にするか、このプロファイルに即して再設定します。

プロファイルでアクティブなセキュリティ、インスペクション ルール、およびリライト ルールを設定したら、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。

アクティブなセキュリティ機能

プロファイルのアクティブなセキュリティ機能は、データ オーバーフロー防御、HTTP ヘッダー処理、および cookie の暗号化/復号化など独自のメッセージ処理およびセキュリティ タスクを実行します。

（注）　ルールまたはシグニチャとは違い、その設定で規定されている場合を除き、アクティブなセキュリティ機能をシステムに追加する、またはカスタマイズすることはできません。

一般的に、監視モードの仮想 Web アプリケーションの場合、ACE Web Application Firewall はセキュリティ ルールをトラフィックに適用しますが、ルールに違反するメッセージを遮断することはありません。監視モードの仮想 Web アプリケーションでは、HTTP ヘッダー処理、HTTP 例外マッピング、および cookie セキュリティなどほとんどのアクティブ セキュリティ機能が有効のままです。しかし、データ オーバーフロー防御および参照元強化は、監視モードに制約されます。つまり起動された場合、イベントはログに記録されますが、メッセージは遮断されません。

一般的に、プロファイルのアクティブなセキュリティ設定を表示または変更するには、操作メニューで [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。アクティブなセキュリティ機能名の横の [view] リンク（組み込みプロファイルの場合）または [edit] リンク（ユーザ作成のプロファイルの場合）をクリックして、その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ます。

HTTP ヘッダー処理

逆プロキシとして、ACE Web Application Firewall はメッセージに含まれる特定の HTTP ヘッダーを自動的に処理して挿入します。たとえばメッセージを処理すると、`Date` ヘッダーおよび `Content-Length` ヘッダーに適切な値を挿入します。しかし、メッセージ内で見つかった他の種類の HTTP ヘッダーは、変更されずに通過します。ヘッダーを通過させるのではなく、ACE Web Application Firewall がメッセージ内の特定のヘッダーの変更、追加、または削除を行うように設定することができます。

HTTP ヘッダーの処理ページには、逆プロキシでの操作が必要なことが多い HTTP ヘッダー（`Server` ヘッダーおよび `X-Forwarded-For` ヘッダーなど）を設定するためのコントロールが用意されています。さらに、名前で識別される任意の HTTP ヘッダーに対して特別な処理を設定できます。HTTP ヘッダー処理は、要求側または応答側のいずれかで指定できます。

特定の種類のヘッダーの値は、ポリシーでは設定できません。一般的に、`Date` ヘッダーおよび `Content-Length` ヘッダーなどのヘッダーは、実行時に決定された値が挿入されます。さらに、ヘッダーの通過は、「ホップバイホップ」ヘッダーと見なされる次のヘッダーには適用されません。これらのヘッダーは、単一のトランスポート層の接続においてだけ重要です。

- Accept-Encoding
- Connection
- Keep-Alive
- Proxy-Authenticate
- Proxy-Authorization
- TE
- Trailers
- Transfer-Encoding
- Upgrade

次の表に、HTTP ヘッダー処理の設定を示します。

表 5-2　HTTP ヘッダー処理の設定

ラベル	説明
[Insert "X-Forwarded-For" header with client's IP address]	逆プロキシ サーバは、多くの場合 `X-Forwarded-For` HTTP ヘッダーを使用してバックエンド システムに対する要求を出したクライアントを識別します。このヘッダーを使用して、要求元として表示された IP アドレスを ACE Web Application Firewall で受信されたようにバックエンド アプリケーションに示します。このヘッダーは、次のオプションのいずれかによって指定されたように追加されます。 • [if the header does not already exist] : メッセージ内にヘッダーが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している場合、ヘッダーは元の値で通過します。 • [replacing any existing value] : 既存のヘッダーを削除し、カスタム ヘッダーを追加します。 • [in addition to any existing value] : メッセージ内にヘッダーがすでに存在するか、存在しないかに関係なく、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内にすでに存在する場合、ヘッダーのインスタンスが 2 つになります。 • [appending to any existing value] : ヘッダーがすでに存在する場合、カンマおよびソースの IP アドレスを既存のヘッダーの末尾に追加します。メッセージにヘッダーが含まれない場合は、ヘッダーが追加されます（このオプションは、特に、広く使用されている Squid オープン ソース Web プロキシで、最適な相互運用性を得るために推奨されます）。
[Insert Client SSL Certificate DN in header named]	メッセージに含まれるクライアント SSL 証明書の対象の Distinguished Name（DN; 識別名）を新しいヘッダーとして挿入します。DN 値は、指定した名前でヘッダーに追加されます。ヘッダーは、次のオプションで指定されたように追加されます。 • [if the header does not already exist] : メッセージ内にヘッダーが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している場合、ヘッダーは元の値で通過します。 • [replacing any existing value] : 既存のヘッダーを削除し、カスタム ヘッダーを追加します。 • [in addition to any existing value] : メッセージ内にヘッダーがすでに存在するか、存在しないかに関係なく、ヘッダーを追加します。存在する場合、このヘッダーのインスタンスが 2 つになります。 • [appending to any existing value] : ヘッダーがすでに存在する場合、カンマおよび証明書の DN を既存のヘッダーの末尾に追加します。メッセージにヘッダーが含まれない場合は、ヘッダーが追加されます このオプションによってヘッダーに追加される証明書の DN 値については、[I/O Process Settings] ページで指定されるように、[SSLVerifyClient] 設定を [optional_no_ca value] に指定する必要があります。設定されていない場合、ヘッダーには空白の値が追加されます。
[Rewrite "Host" header with destination server hostname]	選択した場合、要求内の Host ヘッダー値が、仮想 Web アプリケーションの定義に指定された宛先サーバから得られた宛先バックエンド ホストの名前に置き換えられます。

ラベル	説明
[Custom Header Processing]	要求メッセージの場合、指定の HTTP ヘッダーで次の処理を実行します。次の値を指定することによって、ヘッダー処理を設定します。 • 最初のフィールドに、処理対象のヘッダー名を入力します。 • 次の操作メニューによって、ヘッダーの処理方法が指定されます。 – [strip]：指定した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、ヘッダーの存在を予期したものではありません。ヘッダーが存在しなくても、エラーではありません。 – [set if empty]：指定のヘッダーが存在しない場合、指定された値を挿入します。存在する場合、何も実行しません。その結果生じるメッセージには、設定した名前のヘッダーが少なくとも 1 つ含まれます。 – [replace value]：既存の指定のヘッダーを除去し、ヘッダーの新しいインスタンスを指定した値で挿入します。 – [add value]：指定した名前および値で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。したがって、同じ名前を持つヘッダーが少なくとも 1 つ、場合によっては複数含まれるメッセージが生成されます。 – [append]：同じ名前の既存のヘッダーの末尾にカンマ、設定した値の順に追加します。要求に指定のヘッダーが含まれない場合、値が追加されます。同じ名前の複数のヘッダーが含まれる場合、値は、これらのヘッダーの 1 つの末尾に追加されます。 操作は、インターフェイスに表示される順番に実行されます。 • （[strip] オプションを選択しない場合）、この操作に続くテキストフィールドには、指定する値を入力します。このフィールドは、Reactor 表現形式の動的な値（たとえば $(REQUEST_HEADER['Date']）をサポートします。 Reactor 表現構文に関する詳細については、『*Cisco ACE Web Application Firewall 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 アプリケーションで処理された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、送信応答へと通過します。 または、ACE Web Application Firewall が `Server` ヘッダーをこのフィールドで指定した値にリライトするように設定できます。

ラベル	説明
[Custom Header Processing]	要求応答の場合、指定の HTTP ヘッダーで次の処理を実行します。次の値を指定することによって、ヘッダー処理を設定します。 • 最初のフィールドに、処理対象のヘッダー名を入力します。 • 次の操作メニューによって、ヘッダーの処理方法が指定されます。 – [strip]：指定した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、ヘッダーの存在を予期したものではありません。ヘッダーが存在しなくても、エラーではありません。 – [set if empty]：指定のヘッダーが存在しない場合、指定された値を挿入します。存在する場合、何も実行しません。その結果生じるメッセージには、設定した名前のヘッダーが少なくとも 1 つ含まれます。 – [replace value]：既存の指定のヘッダーを除去し、ヘッダーの新しいインスタンスを指定した値で挿入します。 – [add value]：指定した名前および値でヘッダーの新しいインスタンスを挿入します。同じヘッダー名を持つ既存のヘッダーに影響することはないので、同じヘッダー名が少なくとも 1 つ、場合によっては複数含まれるメッセージが生成されます。 – [append]：同じ名前の既存のヘッダーの末尾にカンマ、設定した値の順に追加します。応答に指定のヘッダーが含まれない場合、値が追加されます。同じ名前の複数のヘッダーが含まれる場合、値は、これらのヘッダーの 1 つの末尾に追加されます。 操作は、インターフェイスに表示される順番に実行されます。 • ([strip] オプションを選択しない場合)、この操作に続くテキストフィールドには、指定するヘッダー値を入力します。

HTTP 例外マッピング

HTTP 例外は、要求処理の過程におけるエラーまたは他の予期しないイベントを示す応答メッセージです。この例外は、要求自体におけるエラーまたはバックエンド システムの処理またはネットワークにおけるエラーから生じることがあります。場合によっては、バックエンド アプリケーションから渡された HTTP 例外に、ハッカーが使用できる Web サーバのスタック トレースなど、潜在的な攻撃者にとっての機密情報が含まれます。Cisco ACE Web Application Firewall で例外をマップすることによって、汎用エラー 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。

例外マッピングが有効な場合、ACE Web Application Firewall は、特定のエラー情報を返すのではなく、ユーザが設定した応答を返します。たとえば 400 や 500 のすべてのエラーを汎用の 500 エラーにマップしたり、一部のエラーに対して特定の応答を設定したりできます。

次の表に、HTTP 例外処理の設定を示します。

表 5-3　HTTP 例外処理の設定

ラベル	説明
[For server errors (status code 400 and above) not specified below]	HTTP ステータス コード 400 以上のバックエンド システムからのすべてのエラー応答を、汎用エラー応答にマップしてクライアントに返すには、このオプションを使用します。デフォルトでは、このような応答はクライアントへと通過します。 HTTP 500 ステータス コードの汎用応答では、「The server encountered an internal error and was unable to complete your request」という記述とともにサーバ エラーが報告されます。 このエラー マッピング オプションは、次に示すカスタム マッピング オプションとともに使用できます。両方が適用されるエラー コードについては、カスタム応答設定がこの汎用マッピングよりも優先されます。 通過に関してこのオプションが設定されており、例外にマップされている特定のステータス コードが存在する場合、クライアントが受信したエラー応答の `Server` ヘッダー値が変わります。ポリシー設定で指定されている場合、マップされたエラーは ACE Web Application Firewall 設定の `Server` 値になりますが、通過したエラーはバックエンド システムによって設定された `Server` 値になります。
[Status Codes]	すべてのエラー応答を汎用応答にマップするのではなく、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] フィールドに、カスタム応答にマップされる応答の数字のエラー コードを入力します。数字は個別に、または「400, 403, 500-599」などの範囲として入力できます。範囲および単一の値は、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、クライアントへの送信のために設定する応答にマップされます。汎用マッピング設定も設定されている場合、この設定が優先されます。
[Status Code]	受信応答からのステータス コードを通過させる、またはプリセットのステータス コードを使用するオプションが設定されている、送信応答メッセージのステータス コード。
[Content-Type]	送信応答メッセージのコンテンツ符号化タイプ。デフォルトでは、text/html です。

ラベル	説明
[Other Headers]	応答に含ませる他のすべての HTTP ヘッダー。 このフィールドでは、一部の HTTP ヘッダーは指定できません。たとえば、Date ヘッダー値および Content-Length ヘッダー値は、バックエンド応答から通過します。手動では指定できません。また、Server ヘッダー値は、バックエンド システムから通過する（デフォルト）か、HTTP ヘッダー処理設定のより具体的な設定によって挿入されます。
[Response Body]	クライアントに送信される HTTP 応答の本文。

参照元強化

参照元 HTTP 要求ヘッダー（つまり、基準ではスペルに誤りがある `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。参照元強化機能は、Cross Site Request Forgery（CSRF; クロス サイト リクエスト フォージェリ）と呼ばれる種類の攻撃から保護できます。

CSRF 攻撃の一般的な例には、オンライン バンキング アプリケーションなど機密性の高い Web アプリケーションへのアクティブなブラウザ セッションを持つユーザが含まれます。認証されたセッションがアクティブな状態の場合、このユーザは別の Web サイトのリンクをクリックするように仕向けられる可能性があります。この Web サイトでは、攻撃者の口座に資金を送金するなど銀行のアプリケーションに対する操作が開始され、この操作が遂行されます。このリンクは、攻撃者が管理する Web サイト上、電子メール内、またはパブリック フォーラムなど他の場所に存在する可能性があります。

このような攻撃は、`Referer` ヘッダーに示されるホストに基づいてメッセージを制限することによって回避できます。参照元値によって識別されるホストが Web アプリケーション自体のホストと異なる場合には、要求を拒否できます。これによって、機密性の高い操作を実行するための要求 URL が第三者の Web サイト上又は電子メール内など他の場所で取得された要求を遮断します。

次の表に、参照元強化の設定を示します。

表 5-4　参照元強化の設定

ラベル	説明
[If the "Referer" header is present, require that its value matches requested host name]	選択した場合、`Referer` ヘッダーが含まれる要求には、要求 URL のホスト名に合致するホスト名を持つ URL を値として持つように要求されます。つまり参照元は、外部アプリケーションまたは Web サイトによってではなく、要求によって対応される Web アプリケーションを識別する必要があります。
[Never check "Referer" header on GET requests]	通常、この種の攻撃では HTTP GET 要求は使用されないので、GET 要求に関する確認を無効にすることができます。確認は、POST 要求または他の HTTP 方式の受信要求に適用されます。
[Monitor Mode]	選択した場合、`Referer` ヘッダーで識別されるホストが要求 URL と合致しないと、このイベントはログに記録されますが、メッセージは許可されます。

HTTP Cookie セキュリティ

多くの場合、Web アプリケーションは HTTP cookie を使用して特定のユーザまたはセッションに関する情報を格納します。サーバは、クライアントに送信される応答に cookie を埋め込み、ブラウザは、以降の要求で cookie を変えずに戻します。cookie は、個人情報を含んだり、セッション ハイジャック攻撃の基盤を形成したりする可能性があります。多くの場合 cookie の内容は、バックエンド アプリケーションによるものを除いて変更されません。

cookie セキュリティが有効であるか、無効であるかに関係なく、メッセージ内の cookie はプロファイルで設定したデータ オーバーフローおよび HTTP ヘッダー処理設定の対象です。cookie セキュリティが有効な場合、ACE Web Application Firewall は cookie 固有の認証方法を適用し、クライアントに送信する前に cookie の暗号化または署名を行うことによって cookie のセキュリティを確保できます。

cookie の処理後、ACE Web Application Firewall がクライアントからの以降の要求で cookie を受信すると、シグニチャを確認するか、cookie を復号化してからバックエンド Web アプリケーションに転送します。これによって ACE Web Application Firewall は、cookie が Firewall からクライアントへの送信時に変更されていないか、または表示されていないかを確認できます。

cookie セキュリティが有効な場合、ACE Web Application Firewall は、シグニチャを確認できない、cookie を復号化できない、または cookie の正確さを検証できないことを根拠に無効と判明した cookie を削除します （cookie セキュリティが無効な場合、cookie は変更されずに ACE Web Application Firewall を通過します）。cookie は、閉じられていない引用符、重複する属性、およびカンマ（","）、セミコロン（";"）、二重引用符（"(")"）、等号（"="）、および空白などの禁じられている文字が含まれている場合に無効と見なされます。

（注） cookie セキュリティは、Javascript を使用してクライアント側で cookie を設定または変更するアプリケーションでは使用しません。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の種類を示すように cookie を設定していることがあります。クライアント側で変更された cookie は検証または復号化でエラーが発生するので、このような場合には cookie セキュリティを無効にする必要があります。cookie シグニチャを有効にした場合、クライアントで追加された新しい cookie は、ゲートウェイでドロップされますが、暗号化を有効にすると、新しい cookie が受け入れられます。いずれの場合でも、クライアントで変更された cookie はドロップされます。

cookie のヘッダー違反は、cookie の暗号化または cookie への署名によって cookie セキュリティが明示的に有効にされている場合に発生します。次の表は、アクティブな cookie セキュリティ機能の設定を示します。

表 5-5　Cookie セキュリティ機能

ラベル	説明
[Sign (HMAC-SHA1)]	応答の cookie にデジタル署名を施してからクライアントに送信し、以降の要求で戻されたときに検証するには、このオプションを選択します。デジタル署名は、cookie の完全性を確保するのに役立ちます。（たとえばセッション スプーフィングを行う意図で）悪意を持って改ざんされた cookie が保護対象アプリケーションに転送されないようにできます。cookie シグニチャが無効な場合、cookie は要求から除去されます。 Cisco ACE Web Application Firewall は、keyed-Hash Message Authentication Code（HMAC; ハッシュ メッセージ認証コード、または KHMAC; 鍵付きハッシュ メッセージ認証コード）を使用して、ポリシー設定のパスフレーズ フィールドで指定した秘密鍵に基づいて cookie に署名します。別の ACE Web Application Firewall クラスタで処理された cookie を持つ要求を受信する可能性のあるすべての ACE Web Application Firewall クラスタでは、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 オーバーフロー防御も使用している場合には、cookie への署名の効果を考慮する必要があります。cookie に署名すると、Cisco ACE Web Application Firewall はアウトバンドのメッセージにヘッダー（シグニチャ cookie）をさらに追加します。このシグニチャの長さは、常に 8 文字です。cookie ヘッダーの名前は、これよりも 3 文字長くなります。したがって元の cookie 値の属性が 10 文字以下の場合、シグニチャ cookie ヘッダーの合計サイズは、元の cookie よりも大きくなります。たとえば、次の cookie について考えてみましょう。 Cookie: NAME=123456789a 署名されると、メッセージには次の形式のシグニチャ cookie（実際のシグニチャではない）が含まれるようになります。 Cookie: NAMESig=12345678 このように、cookie 値は常に 8 文字で示されます。しかし、名前には 3 文字が追加されます。

ラベル	説明
[Encrypt (AES)]	クライアントに送信する前にメッセージ内の cookie を Cisco ACE Web Application Firewall で暗号化するには、このオプションを選択します。クライアントからの以降の要求で暗号化された cookie を受信すると、cookie を復号化してからバックエンド アプリケーションに送信します。 cookie の暗号化には、クライアントからの cookie データを隠す機能があります。cookie は、クライアントおよびサーバで生成できます。（クライアントで生成された cookie であることを示す）暗号化されていない cookie を受信した場合、ACE Web Application Firewall はこの cookie を通過させます。したがって、一般的に暗号化は完全性保護の形式を提供できますが、ACE Web Application Firewall は すべての cookie の暗号化を要求するわけではないので、暗号化に依存して cookie の完全性を強化できないことを覚えておくことが重要です。 Cisco ACE Web Application Firewall は、対称キーベースの暗号化規格である Advanced Encryption Standard（AES; 高度暗号化規格）を使用して cookie 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付きで生成されます。 cookie ヘッダーのサイズに制限を課すことができる、データ オーバーフロー防御も使用している場合には、cookie 暗号化の効果を考慮する必要があります。暗号化では、元の cookie 値のサイズに比例するバイト数によって、cookie のサイズが大きくなります。特に、暗号化された cookie の長さは、次の式を使用して予測できます。cookie は個別に暗号化されるので、cookie の名前および値の長さをそれぞれ確認し、次の 16 の倍数に切り上げます。次に 3 で割り（余りが出たら切り上げ）、4 をかけます。 たとえば、名前が 10 文字の場合は、10 + 1 = 11。16 に切り上げてから 3 で割り、切り上げると 6。6 に 4 をかけて 24 となります。名前/値の長さの例と暗号化後のサイズを次に示します。 • 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]	cookie の暗号化または署名に使用される秘密鍵。入力するパスフレーズの長さは、少なくとも 5 文字にする必要があります。数字、文字、または特殊文字の任意の組み合わせを含むことができます。 パスフレーズの長さは 5 文字で構わないとしても、5 文字よりも著しく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 文字前後の長さにします。 ポリシーが導入されると、Manager は、クラスタ内のすべての Cisco ACE Web Application Firewall にパスフレーズを送信します。個別に管理されるクラスタが、同じクライアントから以降の要求を受信する場合、これらのクラスタは、同じパスフレーズで設定される必要があります。

データ オーバーフロー防御

データ オーバーフロー防御では、メッセージ内の各種属性のサイズまたは数に基づいてセキュリティを設定できます。データ オーバーフロー防御設定に準拠しないメッセージは、遮断されるか、設定可能な重大度レベルでイベントがログに記録されて通過します。

（注）　仮想 Web アプリケーションの処理設定自体が、メッセージ コンポーネントのサイズに影響を及ぼすことがあります。たとえば、cookie の署名または暗号化によって、新しいヘッダーを挿入したり、既存のヘッダーを拡大したりできます。データ オーバーフロー防御は、cookie 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 Cookie セキュリティ」（P.5-10）を参照してください。

次の表に、データ オーバーフロー防御の設定を示します。

表 5-6　データ オーバーフロー防御の設定

ラベル	説明
[Enforce the following data limits on requests]	データ オーバーフロー防御を有効にし、データ オーバーフロー防御の設定を使用可能にするには、このオプションを選択します。
[Maximum Number of HTTP Headers]	メッセージ内で許可される HTTP ヘッダーの数。
[Maximum Size of Any HTTP Header]	任意の HTTP ヘッダーの最大サイズ（バイト単位）。cookie には適用されません。
[Maximum Cookie Size]	任意の HTTP cookie または暗号化された cookie ヘッダーの最大サイズ（バイト単位）。
[Maximum Total HTTP Header Size]	cookie を含む、すべての HTTP ヘッダーの最大サイズ（KB 単位）。
[Maximum Size of Request URL]	要求 URL の最大サイズ（バイト単位）。この値は、要求されたホスト名、リソース、およびすべての URL パラメータを含みます。
[Maximum Size of GET Query String]	URL 内の GET クエリ文字列の最大サイズ（バイト単位）。クエリ文字列は、疑問符記号に続いて要求に表示されます。たとえば、http://hostname/path/page?query_string です。
[Maximum Number of Request Arguments]	GET 要求または POST 要求内の引数の最大数。GET 要求の引数は、URL に対して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。たとえば、http://example.com/path/page?name1=value1&name2=value2 です。 POST 要求の引数は、同様の名前と値のペアとして要求の本文内に表示されます。
[Maximum Size of Any Argument]	POST 要求または GET 要求内の任意の 1 つの引数の最大サイズ（バイト単位）。引数の名前および値のサイズを含みます。
[Maximum Total Size of Request Body]	要求内の POST 本文の最大合計サイズ（バイト単位）。
[Monitor mode]	選択した場合、データ オーバーフロー設定に違反する要求は、設定された重大度レベルでイベントがログに記録されますが、遮断されません。

ラベル	説明
[Event Log]	監視モード時に適用された場合、この動作の起動から生じるログ イベントの重大度レベルを、ルール グループ レベルまたは仮想 Web アプリケーション レベルのいずれかで制御します。 デフォルトでは、これらのイベントは Warning レベルでログに記録されます。しかしこのルールが監視モードで適用される場合、重大度レベルの引き下げが適切なことがあります。
[Response]	メッセージが、データ オーバーフロー防御設定に違反する場合に ACE Web Application Firewall が実行すべき動作。次のオプションがあります。 • ステータス コード 400 の HTTP エラー応答を返す（クライアント エラー）。 • ステータス コード 500 の HTTP エラー応答を返す（サーバ エラー）。 • 設定したカスタム HTTP エラー応答を返す。 • メッセージの許可は、監視モードの場合と同様です。シグニチャ照合イベントは報告されますが、メッセージは許可されて通過します。

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、メッセージ全体に対して動作してメッセージを遮断するか、通過を許可しますが、リライト ルールは、合致したコンテンツを置き換えてメッセージを変更してから通過させます。また、メッセージ インスペクション ルールは要求に対して動作しますが、メッセージ リライト ルールは、応答に対して動作します。

メッセージ リライト ルールは、バックエンド アプリケーションが、ユーザのクレジット カード番号または社会保障番号などの機密情報を送信しないようにするのに役立ちます。リライト ルールのシグニチャに合致する応答部分は、置換文字で置き換えられます。メッセージ リライト ルールは、応答内でシグニチャ パターンの複数のインスタンスを照合できます。

ポリシーで有効になっている場合、仮想 Web アプリケーションが監視モードだけに設定されていてもメッセージが変更されます。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監視モードであるか、有効モードであるかに関係なく発生します。

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に対してコンテンツ置換を設定する場合には、特別な考慮事項が存在します。バックエンド システムによって圧縮された応答を受信した場合、Cisco ACE Web Application Firewall は応答を通過させることができます。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あり、バックエンド システムが応答の圧縮を実行する場合、圧縮された応答の受信を示すのに使用される HTTP ヘッダー（ACCEPT-ENCODING）を送信要求から除去することによって、圧縮されていない応答を Firewall に受信させる必要があります。

ACCEPT-ENCODING ヘッダーが送信要求から削除される、HTTP ヘッダー処理を設定することによって、仮想 Web アプリケーションでヘッダー ストリッピングを指定できます。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 ルールの有効化および設定を行うには、プロファイル内のリライト 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 5-7　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 グループを有効にするか、無効にするか。このオプションを有効にすると、このルール グループのルールが表示されます。ルールは、個別に有効または無効に設定できます。 次のオプションがあります。 • [Enabled]：このルール グループ内のルールは、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。 有効になっているリライト ルールは、仮想 Web アプリケーションが監視モードの場合でも適用されます。
[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]	グループの各リライト ルールを個別に有効または無効にできます。有効にした場合、ルールは、メッセージ トラフィックに適用されます。シグニチャ照合によってルールが起動された場合、合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換されます。文字は、ルールの Rewrite Char. カラムに示されます。このカラムは、[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、潜在的に悪意のあるコンテンツがないかどうか要求を確認します。このルールはシグニチャを使用して、Web アプリケーション宛のメッセージから対象となるコンテンツを識別します。たとえば、コマンド インジェクションまたはクロス サイト スクリプティング攻撃を検出するために、組み込みのメッセージ インスペクション ルールが存在します。コンテンツが検出されると、ACE Web Application Firewall は要求を遮断するか、イベント ログに記録して通過させることができます。

メッセージ インスペクション ルール セットでは、プロファイルで適用される重大度レベルを basic、moderate、または strict に指定できます。重大度レベルは、有効化されるセット内の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有効化されます。たとえば moderate 重大度を選択すると、ルール セット内の moderate および basic のルールが有効になります。特定のレベルではなく、カスタム オプションで有効にするルールを手動で選択できます。

リライト ルールの有効化および設定を行うには、プロファイル内のメッセージ インスペクション ルール グループの横の [edit] ルールをクリックします。インスペクション ルールには次の設定があります。

表 5-8　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 グループを有効にするか、無効にするか。このオプションを有効にすると、特定の重大度レベルでこのルール グループ内のルールが表示されます。 次のオプションがあります。 • [Enabled]：このルール グループ内のルールは、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]：メッセージによっていずれかの有効なルールが起動された場合、ルール設定で指定された重大度レベル（デフォルトでは Warning）でこのイベントがログに記録されますが、メッセージは遮断されません。 • [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は適用されません。
[Level]	適用するグループのルールの重大度レベル。各ルールは、その重大度レベルごとに記載されます。重大度は、通常、ルール内のシグニチャの数またはスコープ、あるいは調査するメッセージのスコープによって異なります。グループの重大度レベルを選択すると、ACE Web Application Firewall は、同じ重大度レベルのグループ内のルールだけを適用するようになります。 重大度レベルを昇順に並べると、basic、moderate、および strict です。有効にするルールを直接選択するには、[Custom] を選択します。
[Exemptions]	[Exemptions] を使用すると、ルールの適用方法を微調整できます。適用外は、一定のシグニチャを評価の対象外にします。メッセージが適用外のシグニチャに合致した場合、この合致は無視されます。たとえば、ユーザ名を示すパラメータ内の単一引用符（'）を検索するシグニチャを除外することは妥当です。パラメータは、/path?lastname=o'neill のような正規値を持つ場合があるからです。 これらの場合は、単一引用符のパターン シグニチャから lastname パラメータを除外できます。カスタム シグニチャでも同じ効果を得られますが、適用外機能を使用すると設定を簡素化できます。 適用外は、ここで実行されるように基本プロファイルで指定できます。または、（ほとんどの場合に適切なように）仮想 Web アプリケーションに対する修飾子のプロファイルで指定できます。 適用外の設定では、要求全体、パラメータ、または HTTP ヘッダーに適用するかどうかという、適用外のスコープを示します。また、特定のシグニチャを除外するのか、またはすべてのシグニチャを除外するのかも示します。 指定のシグニチャでは、シグニチャ識別子でシグニチャを示します。たとえば、次のとおりです。 **In parameter**: lastname **ignore signature**: CrossScriptXSS.52 ポリシーのシグニチャのシグニチャ識別子を取得するには、[Rules & Signatures] ページで [View Signatures] をクリックします。 適用外がメッセージに適用される場合、Limit によって検出される CROSSITESCRIPT.CrosSiteScript1:CrossScriptXSS.52:REQUEST_GETPARAM['firstname'] が情報レベルでログに記録されますが、オーバーライドによって無効化されます。

ラベル	説明
[Event Log]	監視モード時に適用された場合、このルールの起動から生じるログ イベントの重大度レベルを、ルール グループ レベルまたは仮想 Web アプリケーション レベルのいずれかで指定します。 デフォルトでは、これらのイベントは Warning レベルでログに記録されます。しかし、このルールが監視モードで適用される場合、ルールの重大度レベルの引き下げが適切なことがあります。
[Response]	ルール シグニチャに合致した場合にクライアントに返される応答メッセージを設定するために使用します。次のオプションがあります。 • ステータス コード 400 の HTTP エラー応答を返す（クライアント エラー）。 • ステータス コード 500 の HTTP エラー応答を返す（サーバ エラー）。 • 設定したカスタム エラー応答を返す。 • メッセージの許可は、監視モードの場合と同様です。シグニチャ照合イベントは報告されますが、メッセージは許可されて通過します。