CHAPTER 11

アプリケーション セキュリティ

アプリケーション セキュリティを使用すると、セキュリティ ポリシーを作成して、ネットワークおよび Web アプリケーションの使用を制御できます。作成したポリシーを特定のインターフェイスに適用したり、既存のポリシーを複製して新しいポリシーの設定に利用したり、ルータからポリシーを削除したりできます。

アプリケーション ファイアウォールとも呼ばれるアプリケーション セキュリティ機能は、Cisco IOS 12.4(15)T4 で最初にサポートされました。
Cisco Configuration Professional（Cisco CP）は、Cisco IOS 12.4(9)T 以降のリリースをサポートしています。Cisco CP でサポートされているリリースを確認するには、Cisco Configuration Professional のリリース ノートを参照してください。

この章の内容は、次のとおりです。

アプリケーション セキュリティのウィンドウ

アプリケーション セキュリティのウィンドウにあるコントロールを使用すると、ポリシーをインターフェイスに関連付けたり、グローバル設定を行ったり、アプリケーション セキュリティ ポリシーの追加、削除および複製を行ったりできます。アプリケーション セキュリティ ボタンを使用すると、変更を行う必要のあるアプリケーション セキュリティ エリアに迅速に移動できます。

ポリシー名リスト

変更するポリシーをこのリストから選択します。ポリシーが設定されていない場合、このリストは空白です。また、アプリケーション セキュリティのウィンドウには、ルータで使用できるポリシーがないことを通知するメッセージが表示されます。ポリシーを作成するには、［アクション］ボタンをクリックして［追加］を選択します。

アプリケーション セキュリティのボタン

- ［アクション］ボタン ― ポリシーの追加、選択したポリシーの削除、または選択したポリシーの複製を行う場合にクリックします。ルータにポリシーが設定されていない場合、利用可能なアクションは［追加］だけです。
- ［関連付け］ボタン ― ポリシーをインターフェイスに関連付けることのできるダイアログを表示する場合にクリックします。このダイアログでは、インターフェイスの選択、およびポリシーを適用するトラフィックの方向の指定が可能です。
- ［グローバル設定］ボタン ― すべてのポリシーに適用するタイムアウト値およびしきい値を設定する場合にクリックします。詳細については、「グローバル設定」を参照してください。

電子メール ボタン

電子メール アプリケーションのセキュリティ設定を変更する場合にクリックします。詳細については、「電子メール」を参照してください。

インスタント メッセージング ボタン

Yahoo Messenger や MSN Messenger などのインスタント メッセージング アプリケーションのセキュリティ設定を変更する場合にクリックします。詳細については、「インスタント メッセージング」を参照してください。

ピアツーピア ボタン

KaZa A や eDonkey などのピアツーピア アプリケーションのセキュリティ設定を変更する場合にクリックします。詳細については、「アプリケーション / プロトコル」を参照してください。

URL フィルタリング ボタン

アプリケーション セキュリティ ポリシーでフィルタにかける URL のリストを追加する場合にクリックします。フィルタリング サーバを追加することもできます。

HTTP ボタン

HTTP のセキュリティ設定を変更する場合にクリックします。詳細については、「HTTP」を参照してください。

アプリケーション / プロトコル ボタン

他のアプリケーションおよびプロトコルのセキュリティ設定を変更する場合にクリックします。詳細については、「アプリケーション / プロトコル」を参照してください。

アプリケーションセキュリティーポリシーがない場合

［アプリケーション セキュリティ］タブをクリックしたとき、ルータにアプリケーション セキュリティ ポリシーが設定されていない場合はこのウィンドウが表示されます。このウィンドウではポリシーを作成できます。また、ポリシーの作成時に設定できるパラメータにデフォルト値を指定するグローバル設定を表示できます。

ポリシー名

ルータに設定されているポリシーがない場合は空です。［アクション］コンテキスト メニューから［追加］を選択すると、ポリシー名を作成し、そのポリシーの設定を開始できます。

アクション

ルータにポリシーが設定されていない場合、コンテキスト メニューから［追加］を選択してポリシーを作成できます。ポリシーが設定されると、他のアクション（［編集］と［削除］）も使用できるようになります。

関連付け

ポリシーが設定されていない場合、このボタンは無効です。ポリシーが作成されたら、このボタンをクリックして、そのポリシーをインターフェイスに関連付けることができます。詳細については、「ポリシーをインターフェイスに関連付ける」を参照してください。

グローバル設定

グローバル設定では、ポリシーのパラメータに、タイムアウトやしきい値などのデフォルト値を指定します。Cisco CP では、各パラメータにデフォルト値が用意されており、それぞれの値を変更して新しいデフォルト値を定義できます。特定のアプリケーションやプロトコルで他の値が優先されない限り、この新しいデフォルト値が適用されます。ポリシーの作成時には、特定のパラメータでデフォルト値をそのまま使用するか、別の設定値を選択することができます。デフォルト値はアプリケーション セキュリティの設定ウィンドウには表示されないため、このボタンをクリックして、［グローバル タイムアウトおよびしきい値］ウィ

ンドウで表示する必要があります。詳細については、「インスペクション パラメータ マップと CBAC のタイムアウトおよびしきい値」を参照してください。

電子メール

検査する電子メール アプリケーションをこのウィンドウで指定します。［アプリケーション セキュリティ］タブで使用可能なボタンの詳細については、「アプリケーション セキュリティのウィンドウ」を参照してください。

編集ボタン

選択したアプリケーションの設定を編集する場合にクリックします。ここで設定した値は、ルータに設定されたグローバル設定よりも優先されます。

アプリケーション カラム

電子メール アプリケーションの名前（*bliff*、*esmtp*、*smtp* など）。アプリケーションの設定を編集するには、アプリケーション名の左側にあるチェック ボックスを選択して、［編集］をクリックします。

アラート、監査、タイムアウトの各カラム

これらのカラムには、アプリケーションに対して明示的に設定された値が表示されます。アプリケーションに対して設定が変更されていない場合、このカラムは空です。たとえば、bliff アプリケーションに対して監査が有効に設定され、アラートとタイムアウトの設定は変更されていない場合、［監査］カラムには *オン* と表示され、［アラート］カラムと［タイムアウト］カラムは空白になります。

オプション カラム

選択したアプリケーションに対して他の設定が存在する場合、このカラムにフィールドが表示されることがあります。

最大データ フィールド

簡易メール転送プロトコル（SMTP）の 1 回のセッションで転送できる最大バイト数（データ）を指定します。最大値を超過すると、ファイアウォールによりアラート メッセージがログに記録され、セッションが終了されます。デフォルト値は 20MB です。

セキュリティ保護されたログイン チェック ボックス

セキュリティ保護されていない場所にいるユーザが、認証に暗号化を使用するようにします。

リセット

認証が完了する前にクライアントが protocol 以外のコマンドを入力した場合、TCP 接続をリセットします。

ルータ トラフィック

ルータを宛先または送信元とするトラフィックを検査できるようにします。適用できるプロトコルは、H.323、TCP、UDP だけです。

インスタント メッセージング

このウィンドウでは、Yahoo Messenger や MSN Messenger などのインスタント メッセージング（IM）アプリケーションのトラフィックを制御します。［アプリケーション セキュリティ］タブで使用可能なボタンの詳細については、「アプリケーション セキュリティのウィンドウ」を参照してください。

このウィンドウで指定した特性を持つトラフィックが見つかったときにルータが実行するアクションを指定する方法については、「許可、ブロックする、アラームの各コントロール」を参照してください。

次の例は、Yahoo Messenger のトラフィックに対してブロックされたトラフィック、およびそのアプリケーションのトラフィックが到達したときに生成されるアラームを示しています。

```
Yahoo Messenger        Block          Send Alarm (checked)
```

IM アプリケーションをブロックするものが SDM_HIGH プロファイルです。ルータが SDM_HIGH プロファイルを使用しているのに、そのプロファイルが IM アプリケーションをブロックしない場合は、そのアプリケーションが、プロファイルに指定されていない新しいサーバに接続した可能性が考えられます。ルータがそのようなアプリケーションをブロックできるようにするには、IM アプリケーションの横にある［アラームを送信する］チェック ボックスを選択して、そのアプリケーションが接続しているサーバの名前を明らかにします。そして、CLI を使用して、そのサーバからのトラフィックをブロックします。次の例では、サーバ名として newserver.yahoo.com を使用しています。

```
Router(config)# appfw policy-name SDM_HIGH
Router(cfg-appfw-policy)# application im yahoo
Router(cfg-appfw-policy-ymsgr)# server deny name newserver.yahoo.com
Router(cfg-appfw-policy-ymsgr)# exit
Router(cfg-appfw-policy)# exit
Router(config)#
```

（注）
- IM アプリケーションは、HTTP などのノンネイティブのプロトコル ポートや、ネイティブの TCP および UDP ポートを介して通信できます。Cisco CP では、アプリケーションのネイティブ ポートに基づいて、ブロックおよび許可のアクションが設定され、HTTP ポートを介して実行される通信は常にブロックされます。
- MSN Messenger 7.0 など、一部の IM アプリケーションでは、デフォルトで HTTP ポートを使用します。これらのアプリケーションを許可するには、IM アプリケーションがそのネイティブ ポートを使用するように設定します。

ピアツーピア アプリケーション

このページでは、Gnutella、BitTorrent、eDonkey などのピアツーピア アプリケーションにポリシー設定を作成できます。［アプリケーション セキュリティ］タブで使用可能なボタンの詳細については、「アプリケーション セキュリティのウィンドウ」を参照してください。

このウィンドウで指定した特性を持つトラフィックが見つかったときにルータが実行するアクションを指定する方法については、「許可、ブロックする、アラームの各コントロール」を参照してください。

次の例は、BitTorrent のトラフィックに対してブロックされたトラフィック、およびそのアプリケーションのトラフィックが到達したときに生成されるアラームを示しています。

例 11-1　BitTorrent トラフィックのブロック

```
BitTorrent              Block
```

（注）

- ピアツーピア アプリケーションは、HTTP などのノンネイティブのプロトコル ポートや、ネイティブの TCP および UDP ポートを介して通信できます。Cisco CP では、アプリケーションのネイティブ ポートに基づいて、ブロックおよび許可のアクションが設定され、HTTP ポートを介して実行される通信は常にブロックされます。
- アプリケーション セキュリティ ポリシーでは、altnet.com などの有料サービスから提供されたファイルはブロックされませんが、ピアツーピア ネットワークからダウンロードされたファイルはブロックされます。

URL フィルタリング

URL フィルタリングでは、URL リストを使用して、インターネット Web サイトへのユーザ アクセスを制御できます。URL リストでは、URL を許可するか拒否するかを指定できます。アプリケーション セキュリティ ポリシーに URL フィルタリング機能を追加するには、このウィンドウで［URL フィルタリングの有効化］をクリックします。

ルータにローカル URL リストを 1 つ設定して、すべてのアプリケーション セキュリティ ポリシーに使用することができます。URL リストは、ルータが接続可能な URL フィルタ サーバに保存することもできます。これらのサーバに関する情報は、URL フィルタ サーバ リストに保存されます。ルータに URL フィルタ サーバ リストを 1 つ設定して、すべてのアプリケーション セキュリティ ポリシーに使用することができます。

このウィンドウでローカル URL リストを管理するには、［URL の追加］、［URL の編集］、および［URL リストのインポート］の各ボタンを使用します。Cisco IOS ソフトウェアでは、アプリケーション セキュリティ ポリシーが設定されているかどうかに関係なく、これらのリストを管理できるため、［追加タスク］ウィンドウでこれらのリストを管理することもできます。

ローカル URL リストを管理する方法については、「ローカル URL リスト」を参照してください。

URL フィルタ サーバ リストを管理する方法については、「URL フィルタ サーバ」を参照してください。

ルータでローカル URL リストと URL フィルタ サーバ上の URL リストを組み合せて使用する方法については、「URL フィルタリングの優先順位」を参照してください。

URL フィルタリングの一般情報については、「URL フィルタリング ウィンドウ」を参照してください。

HTTP

このウィンドウでは、HTTP トラフィック検査の全般的な設定を指定します。[アプリケーション セキュリティ] タブで使用可能なボタンの詳細については、「アプリケーション セキュリティのウィンドウ」を参照してください。

このウィンドウで指定した特性を持つトラフィックが見つかったときにルータが実行するアクションを指定する方法については、「許可、ブロックする、アラームの各コントロール」を参照してください。

ルータによる HTTP トラフィック検査の詳細については、次のリンク先にある『HTTP Inspection Engine』を参照してください。

http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a0080455acb.html

非準拠の HTTP トラフィックを検出するチェック ボックス

HTTP プロトコルに準拠していないパケットの HTTP トラフィックを検査する場合に選択します。[許可]、[ブロックする]、[アラーム] の各コントロールを使用して、このタイプのトラフィックが見つかったときにルータが実行するアクションを指定します。

（注） 非準拠の HTTP トラフィックをブロックすると、コンテンツに応じてブロックされていない可能性のある、よく利用される Web サイトが HTTP プロトコルに準拠していない場合、その Web サイトからのトラフィックをルータが破棄する場合があります。

トンネリング アプリケーションを検出するチェック ボックス

トンネリング アプリケーションによって生成されたパケットの HTTP トラフィックを検査する場合に選択します。[許可]、[ブロックする]、[アラーム] の各コントロールを使用して、このタイプのトラフィックが見つかったときに Cisco CP が実行するアクションを指定します。

URI の最大長の検査を設定するチェック ボックス

Universal Resource Indicator（URI）の最大長を定義する場合に選択します。最大長をバイト単位で指定し、[許可]、[ブロックする]、[アラーム] の各コントロールを使用して、この値より長い URL が見つかったときにルータが実行するアクションを指定します。

HTTP の検査を有効にするチェック ボックス

ルータで HTTP トラフィックを検査する場合に選択します。Java アプリケーションからのトラフィックをブロックする場合は、[...] ボタンをクリックし、既存の ACL を指定するか、Java 検査用に新しい ACL を作成して、Java ブロッキング フィルタを指定できます。

HTTPS の検査を有効にするチェック ボックス

ルータで HTTPS トラフィックを検査する場合に選択します。

タイムアウト値を設定するチェック ボックス

HTTP セッションのタイムアウトを設定する場合に選択し、[タイムアウト] フィールドに秒数を入力します。この時間を超過したセッションは破棄されます。

監査証跡を有効にする

HTTP トラフィックに CBAC 監査証跡を設定できます。この設定は、[グローバル タイムアウトおよびしきい値] ウィンドウの設定よりも優先されます。[デフォルト] は、現在のグローバル設定が使用されるという意味です。[オン] を選択すると、HTTP トラフィックで CBAC 監査証跡を明示的に有効にできます。HTTPS 検査が有効になっている場合は、HTTPS トラフィックでも CBAC 監査証跡が有効になります。この設定は、監査証跡のグローバル設定よりも優先されます。[オフ] を選択すると、HTTP トラフィックで CBAC 監査証跡を明示的に無効にできます。HTTPS 検査が有効になっている場合は、HTTPS トラフィックでも CBAC 監査証跡が無効になります。この設定は、監査証跡のグローバル設定よりも優先されます。

ヘッダーのオプション

HTTP ヘッダーの長さ、およびヘッダーに含まれている要求方式に基づいて、ルータがトラフィックを許可または拒否するように指定できます。この要求方式は、URL や Web ページの取得などのアクションを実行するために、HTTP サーバに送信されるコマンドです。［アプリケーション セキュリティ］タブで使用可能なボタンの詳細については、「アプリケーション セキュリティのウィンドウ」を参照してください。

最大ヘッダー長を設定するチェック ボックス

HTTP ヘッダーの長さに基づいて、ルータがトラフィックを許可または拒否するように指定する場合に選択し、要求および応答の最大ヘッダー長を指定します。［許可］、［ブロックする］、［アラーム］の各コントロールを使用して、ヘッダー長がこれらの値を超過したときにルータが実行するアクションを指定します。

拡張要求方式の設定チェック ボックス

拡張要求方式に基づいて、ルータが HTTP トラフィックを許可または拒否するように指定する場合は、その要求方式の横にあるチェック ボックスを選択します。［許可］、［ブロックする］、［アラーム］の各コントロールを使用して、その要求方式を使用したトラフィックが見つかったときにルータが実行するアクションを指定します。

RFC 要求方式の設定チェック ボックス

RFC 2616（*Hypertext Transfer Protocol — HTTP/1.1*）で指定された HTTP 要求方式のいずれかに基づいて、ルータが HTTP トラフィックを許可または拒否するように指定する場合は、その要求方式の横にあるチェック ボックスを選択します。［許可］、［ブロックする］、［アラーム］の各コントロールを使用して、その要求方式を使用したトラフィックが見つかったときにルータが実行するアクションを指定します。

コンテンツのオプション

ルータが HTTP トラフィックのコンテンツを検査し、トラフィックを許可または拒否するように指定できます。また、ルータによる確認事項に応じてアラームが生成されるように指定することもできます。［アプリケーション セキュリティ］タブで使用可能なボタンの詳細については、「アプリケーション セキュリティのウィンドウ」を参照してください。

このウィンドウで指定した特性を持つトラフィックが見つかったときにルータが実行するアクションを指定する方法については、「許可、ブロックする、アラームの各コントロール」を参照してください。

コンテンツ タイプを検証するチェック ボックス

応答と要求の照合、不明なコンテンツ タイプに対するアラームの有効化、またはこの両方の方式を使用することによって、ルータが HTTP パケットのコンテンツを検証するように指定する場合に選択します。［許可］、［ブロックする］、［アラーム］の各コントロールを使用して、要求と応答が照合できないとき、また不明なコンテンツ タイプが見つかったときにルータが実行するアクションを指定します。

コンテンツの長さを設定するチェック ボックス

HTTP パケットのデータに最小長と最大長を指定する場合は、このチェック ボックスを選択し、各フィールドに値を入力します。［許可］、［ブロックする］、［アラーム］の各コントロールを使用して、データの量が最小長を下回る場合、または最大長を上回る場合にルータが実行するアクションを指定します。

変換時の符号化方式の設定チェック ボックス

パケット内のデータの符号化方式をルータに検証させる場合は、このチェック ボックスを選択し、［許可］、［ブロックする］、［アラーム］の各コントロールを使用して、選択した転送時の符号化方式が見つかったときにルータが実行するアクションを指定します。

Chunk チェック ボックス

RFC 2616（Hypertext Transfer Protocol — HTTP/1）で指定された符号化方式。メッセージの本文は一連の塊で転送され、それぞれの塊には独自のサイズ インジケータが含まれています。

Compress チェック ボックス

UNIX の "compress" ユーティリティで作成された符号化方式。

Deflate チェック ボックス

RFC 1950（ZLIB Compressed Data Format Specification version 3.3）で定義された "ZLIB" 方式と、RFC 1951（DEFLATE Compressed Data Format Specification version 1.3）で定義された "deflate" 圧縮メカニズムを組み合わせたもの。

gzip チェック ボックス

GNU zip（gzip）プログラムで作成された符号化方式。

Identity チェック ボックス

デフォルトの符号化方式で、符号化が行われていないことを示します。

アプリケーション / プロトコル

このウィンドウでは、他のウィンドウには見つからないアプリケーションやプロトコルにポリシー設定を作成できます。［アプリケーション セキュリティ］タブで使用可能なボタンの詳細については、「アプリケーション セキュリティのウィンドウ」を参照してください。

アプリケーション / プロトコル ツリー

［アプリケーション / プロトコル］ツリーを使用すると、表示するアプリケーションやプロトコルのタイプに応じて、右側のリストにフィルタを適用できます。まず、表示する一般的なタイプのブランチを選択します。右側のフレームには、選択したタイプの選択可能な項目が表示されます。ブランチの左側にプラス（+）記号が表示されている場合は、フィルタの絞り込みに使用できるサブカテゴリがあります。+ 記号をクリックしてブランチを開いてから、表示するサブカテゴリを選択します。右側のリストが空白の場合は、そのタイプで選択可能なアプリケーションもプロトコルもありません。アプリケーションを選択するには、ツリーまたはリストで、そのアプリケーションの横にあるチェック ボックスを選択します。

例：シスコのアプリケーションをすべて表示する場合は、ブランチの［Applications］フォルダをクリックしてから、［Cisco］フォルダをクリックします。アプリケーションが、*clp*、*cisco-net-mgmt*、*cisco-sys* のように表示されます。

編集ボタン

選択したアプリケーションの設定を編集する場合は、このボタンをクリックします。ここで設定した値は、ルータに設定されたグローバル設定よりも優先されます。

アプリケーション カラム

アプリケーションまたはプロトコルの名前（*tcp*、*smtp*、*ms-sna* など）。アプリケーションまたはプロトコルの設定を編集するには、そのアプリケーション名またはプロトコル名の左側にあるチェック ボックスを選択して、［編集］をクリックします。

アラート、監査、タイムアウトの各カラム

これらのカラムには、アプリケーションまたはプロトコルに対して明示的に設定された値が表示されます。アプリケーションまたはプロトコルに対して設定が変更されていない場合、このカラムは空です。たとえば、ms-sna アプリケーションに対して監査が有効に設定され、アラートとタイムアウトの設定は変更されていない場合、［監査］カラムには *オン* と表示されますが、［アラート］カラムと［タイムアウト］カラムは空白になります。

オプション カラム

選択したアプリケーションまたはプロトコルに対して他の設定が行われている場合、このカラムにフィールドが表示されることがあります。

最大データ

簡易メール転送プロトコル（SMTP）の 1 回のセッションで転送できる最大バイト数（データ）を指定します。最大値を超過すると、ファイアウォールによりアラート メッセージがログに記録され、セッションが終了されます。デフォルト値は 20MB です。

セキュリティ保護されたログイン

セキュリティ保護されていない場所にいるユーザが、認証に暗号化を使用するようにします。

リセット

認証が完了する前にクライアントが protocol 以外のコマンドを入力した場合、TCP 接続をリセットします。

ルータ トラフィック

ルータを宛先または送信元とするトラフィックを検査できるようにします。適用できるプロトコルは、H.323、TCP、UDP だけです。

インスペクション パラメータ マップと CBAC のタイムアウトおよびしきい値

以下の情報は、検査目的に使用するパラメータ マップを作成または編集する場合、またはコンテキストベース アクセス コントロール（CBAC）のグローバル タイムアウトとしきい値を設定する場合に有用です。CBAC では、タイムアウトとしきい値に基づいて、セッションの状態情報を管理する期間や完全に確立されていないセッションを破棄するタイミングを決定します。これらのタイムアウトとしきい値はすべてのセッションに適用されます。

グローバル タイマー値は、秒、分、または時間単位で指定できます。

TCP 接続タイムアウト値

TCP 接続の確立を待機する時間を指定します。デフォルト値は 30 秒です。

TCP FIN-wait タイムアウト値

ファイアウォールによって FIN 交換が検出された時点から TCP セッションの管理を維持する時間を指定します。デフォルト値は 5 秒です。

TCP アイドル タイムアウト値

アクティビティが検出されなくなった時点から TCP セッションの管理を維持する時間を指定します。デフォルト値は 3,600 秒です。

UDP アイドル タイムアウト値

アクティビティが検出されなくなった時点から UDP（ユーザ データグラム プロトコル）セッションの管理を維持する時間を指定します。デフォルト値は 30 秒です。

DNS タイムアウト値

アクティビティが検出されなくなった時点からドメイン ネーム システム（DNS）の名前検索セッションの管理を維持する時間を指定します。デフォルト値は 5 秒です。

SYN フラッド Dos 攻撃しきい値

ハーフオープン セッションの数が異常に多い場合は、サービス拒否（DoS）攻撃が行われている可能性があります。DoS 攻撃しきい値を設定すると、ルータは、ハーフオープン セッションの合計数が最大しきい値を超えた時点でそれらのセッションの破棄を開始します。次のしきい値を定義することによって、ルータがハーフオープン セッションの破棄を開始するタイミングと停止するタイミングを指定できます。

1 分間のセッション数のしきい値。次のフィールドでは、新しい接続試行数のしきい値を指定します。

下限　新しい接続の数がこの値以下になると、新しい接続の破棄を停止します。デフォルト値は 400 セッションです。

上限　新しい接続の数がこの値を超えると、新しい接続の破棄を開始します。デフォルト値は 500 セッションです。

最大インコンプリート セッション数のしきい値。次のフィールドでは、既存のハーフオープン セッションの合計数のしきい値を指定します。

下限　新しい接続の数がこの値以下になると、新しい接続の破棄を停止します。12.4(11)T よりも前の Cisco IOS でのデフォルト値は 400 セッションです。［下限］値が明示的に設定されていない場合、セッション数が 400 になると、Cisco IOS は新しいセッションの破棄を中止します。

Cisco IOS 12.4(11)T 以降では、デフォルト値は設定されていません。［下限］値が明示的に設定されていない場合、新しい接続の破棄は中止されません。

上限　新しい接続の数がこの値を超えると、新しい接続の破棄を開始します。12.4(11)T よりも前の Cisco IOS でのデフォルト値は 500 セッションです。［上限］値が明示的に設定されていない場合、確立された新しいセッションが 500 を超えると、Cisco IOS はセッションを破棄し始めます。

12.4(11)T 以降の Cisco IOS リリースでは、デフォルト値は設定されていません。［上限］値が明示的に設定されていない場合、新しい接続の破棄は開始されません。

ホストあたりの最大インコンプリート TCP セッション数：

ルータは、1 台のホストに対するハーフオープン セッションの合計数がこの数を超えると、それらのセッションの破棄を開始します。デフォルトのセッション数は 50 です。［ブロック時間］フィールドに値を入力すると、ルータはそのホストに対する新しい接続を指定した時間（分数）だけブロックします。

グローバルに監査を有効にする

すべてのトラフィック タイプに対する CBAC 監査証跡メッセージの生成を有効にする場合に選択します。

グローバルにアラートを有効にする

すべてのトラフィック タイプに対する CBAC アラート メッセージの生成を有効にする場合に選択します。

ポリシーをインターフェイスに関連付ける

このウィンドウでは、選択したポリシーを適用するインターフェイスを選択します。また、ポリシーを適用するトラフィックの方向を、受信、送信、その両方、のいずれにするかを指定できます。

たとえば、ルータに FastEthernet 0/0 と FastEthernet 0/1 のインターフェイスがあり、両方向のトラフィックで FastEthernet 0/1 インターフェイスにポリシーを適用する場合は、FastEthernet 0/1 の横にあるチェック ボックスを選択し、［受信］カラムと［送信］カラム両方のチェック ボックスを選択します。受信トラフィックだけを検査する場合は、［受信］カラムのチェック ボックスだけを選択します。

インスペクション ルールの編集

このウィンドウでは、アプリケーションのカスタム インスペクション ルール設定を指定します。ここで設定し、ルータの設定に適用する値は、グローバル設定よりも優先されます。

このウィンドウで設定できるパラメータのグローバル設定を表示するには、［アプリケーション セキュリティ］ウィンドウの［グローバル設定］ボタンをクリックします。詳細については、「インスペクション パラメータ マップと CBAC のタイムアウトおよびしきい値」を参照してください。

アラート フィールド

次のいずれかの値を選択します。

- ［デフォルト］— アラートのグローバル設定を使用する。
- ［オン］— このタイプのトラフィックが見つかったときに、アラートを生成する。
- ［オフ］— このタイプのトラフィックが見つかったときに、アラートを生成しない。

監査フィールド

次のいずれかの値を選択します。

- ［デフォルト］— 監査証跡のグローバル設定を使用する。
- ［オン］— このタイプのトラフィックが見つかったときに、監査証跡を生成する。
- ［オフ］— このタイプのトラフィックが見つかったときに、監査証跡を生成しない。

タイムアウト フィールド

アクティビティが検出されなくなった時点から、このアプリケーションのセッションの管理を維持する秒数を入力します。TCP アプリケーションならば TCP アイドル タイムアウト値、UDP アプリケーションならば UDP タイムアウト値が、入力したタイムアウト値によって設定されます。

その他のオプション

これ以外のオプションを設定できるアプリケーションもあります。アプリケーションによっては、次に説明するオプションが表示される場合もあります。

最大データ フィールド

簡易メール転送プロトコル（SMTP）の 1 回のセッションで転送できる最大バイト数（データ）を指定します。最大値を超過すると、ファイアウォールによりアラート メッセージがログに記録され、セッションが終了されます。デフォルト値は 20MB です。

セキュリティ保護されたログイン チェック ボックス

セキュリティ保護されていない場所にいるユーザが、認証に暗号化を使用するようにします。

リセット チェック ボックス

認証が完了する前にクライアントが protocol 以外のコマンドを入力した場合、TCP 接続をリセットします。

ルータ トラフィック チェック ボックス

ルータを宛先または送信元とするトラフィックを検査できるようにします。適用できるプロトコルは、H.323、TCP、UDP だけです。

許可、ブロックする、アラームの各コントロール

［許可］、［ブロックする］、［アラーム］の各コントロールを使用して、指定した特性を持つトラフィックが見つかったときにルータが実行するアクションを指定します。これらのコントロールを備えたオプションにポリシーを設定するには、そのオプションの横にあるチェック ボックスを選択します。そして、［アクション］カラムで、そのオプションに関連するトラフィックを許可する場合は［許可］、拒否する場合は［ブロックする］を選択します。このタイプのトラフィックが見つかったときにアラームを送信する場合は、［アラームを送信する］チェック ボックスを選択します。この［アラームを送信する］コントロールは、すべてのウィンドウで使用されるわけではありません。

アプリケーション セキュリティがログにアラームを送信するようにするには、ロギングを有効にしておく必要があります。詳細については、「アプリケーション セキュリティ ログ」を参照してください。