CHAPTER 39

URL フィルタリング

URL フィルタリングでは、URL リストの情報に基づいて、インタネット上の特定の Web サイトへのアクセスを許可または拒否することにより、その Web サイトへのアクセスを制御できます。ルータ上でローカル URL リストを管理することも、Websense または Secure Computing URL フィルタ リスト サーバ上の URL リストを使用することもできます。URL フィルタリングは、URL フィルタリングを有効にするアプリケーション セキュリティ ポリシーを設定することによって有効になります。

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くても、URL フィルタリングを有効にするポリシーが作成された場合に URL フィルタリングに使用できる、ローカル URL リストと URL フィルタ サーバ リストを管理できます。

この章の内容は、次のとおりです。

- URL フィルタリング ウィンドウ
- ローカル URL リスト
- URL フィルタ サーバ

URL フィルタリングの詳細については、次のリンクを参照してください。

ファイアウォール Websense URL フィルタリング

URL フィルタリング ポリシーの使用方法については、「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 ウィンドウ

このウィンドウには、ルータの URL フィルタリングのグローバル設定が表示されます。ローカル URL リストと URL フィルタ サーバ リストは、［追加タスク］画面または［アプリケーション セキュリティ］ウィンドウで管理できます。URL フィルタリングのグローバル設定は、［追加タスク］ウィンドウにおいてのみ管理できます。設定値を変更するには、［グローバル設定の編集］ボタンを使用してください。

このウィンドウに表示される各設定の説明については、「グローバル設定の編集」を参照してください。

Cisco CP で提供される URL フィルタリング機能の説明については、「URL フィルタリング」の概略情報を参照してください。

グローバル設定の編集

このウィンドウでは、URL フィルタリングのグローバル設定を編集します。

（注）　ルータのロギングを有効にして、URL フィルタ アラート、監査追跡メッセージ、および URL フィルタ サーバに関連するシステム メッセージが報告されるようにする必要があります。

許可モード

このボックスを選択すると、ルータがサーバ リスト内のいずれの URL フィルタ サーバとも接続できない場合に許可モードになります。ルータが許可モードになっていると、ルータが URL フィルタ サーバ リスト内のいずれのサーバとも接続できない場合に、すべての HTPP リクエストの通過が許可されます。デフォルトでは、許可モードは無効に設定されています。

URL フィルタ アラート

このボックスを選択すると、ルータによる URL フィルタリング アラート メッセージのログが有効になります。URL フィルタリング アラート メッセージでは、URL フィルタ サーバが停止した、HTTP リクエストの中に検索要求には長すぎる URL が含まれている、などのイベントが報告されます。このオプションはデフォルトで無効になっています。

監査証跡

このボックスを選択すると、ルータによる監査追跡のログが有効になります。ルータでは、HTTP リクエストの許可 / 拒否を示す URL 要求ステータス メッセージやその他の監査追跡メッセージが記録されます。このオプションはデフォルトで無効になっています。

URL フィルタ サーバ ログ

このボックスを選択すると、ルータによる URL フィルタ サーバ関連のシステム メッセージのログが有効になります。このオプションはデフォルトで無効になっています。

キャッシュ サイズ

直近に要求された IP アドレスと、それぞれに対応する許可ステータスを保存するキャッシュの最大サイズを設定できます。このキャッシュのデフォルト サイズは、5,000 バイトです。0 ～ 2,147,483,647 バイトを指定できます。キャッシュは、12 時間ごとにクリアされます。

バッファリングされる HTTP 要求の最大数

ルータにバッファされる未処理の HTTP リクエストの最大数を設定できます。デフォルトでは、最大 1,000 のリクエストがルータにバッファされます。1 ～ 2,147,483,647 のリクエストを指定できます。

バッファリングされる HTTP 応答の最大数

ルータにバッファされる、URL フィルタ サーバからの HTTP レスポンスの数を設定できます。この数値に到達すると、ルータではそれ以上のレスポンスが破棄されます。デフォルト値は 200 です。0 ～ 20000 の値を設定できます。

URL フィルタリングの全般設定

URL フィルタ名の指定、URL フィルタで一致が検出されたときに実行されるルータの処理の指定、ログおよびキャッシュ サイズのパラメータの設定を行います。URL フィルタリングのパラメータ マップをすべてのルータ インターフェイスに適用するわけではない場合は、送信元インターフェイスを指定することもできます。

URL フィルタ名

URL フィルタの設定方法や使用方法を示す名前を入力します。たとえば、Fast Ethernet 1 の送信元インターフェイスを指定する場合は、「fa1-parmap」という名前を入力できます。また、URL フィルタで IP アドレス 192.128.54.23 の Websense URL フィルタ サーバが使用される場合は、「websense23-parmap」という名前を入力できます。

許可モード

このボックスを選択すると、ルータがサーバ リスト内のいずれの URL フィルタ サーバとも接続できない場合に許可モードになります。ルータが許可モードになっていると、ルータが URL フィルタ サーバ リスト内のいずれのサーバとも接続できない場合に、すべての HTPP リクエストの通過が許可されます。デフォルトでは、許可モードは無効に設定されています。

URL フィルタ アラート

このボックスを選択すると、ルータによる URL フィルタリング アラート メッセージのログが有効になります。URL フィルタリング アラート メッセージでは、URL フィルタ サーバが停止した、HTTP リクエストの中に検索要求には長すぎる URL が含まれている、などのイベントが報告されます。このオプションはデフォルトで無効になっています。

監査証跡

このボックスを選択すると、ルータによる監査追跡のログが有効になります。ルータでは、HTTP リクエストの許可 / 拒否を示す URL 要求ステータス メッセージやその他の監査追跡メッセージが記録されます。このオプションはデフォルトで無効になっています。

URL フィルタ サーバ ログ

このボックスを選択すると、ルータによる URL フィルタ サーバ関連のシステム メッセージのログが有効になります。このオプションはデフォルトで無効になっています。

キャッシュ サイズ

直近に要求された IP アドレスと、それぞれに対応する許可ステータスを保存するキャッシュの最大サイズを設定できます。このキャッシュのデフォルト サイズは、5,000 バイトです。0 ～ 2,147,483,647 バイトを指定できます。キャッシュは、12 時間ごとにクリアされます。

バッファリングされる HTTP 要求の最大数

ルータにバッファされる未処理の HTTP リクエストの最大数を設定できます。デフォルトでは、最大 1,000 のリクエストがルータにバッファされます。1 ～ 2,147,483,647 のリクエストを指定できます。

バッファリングされる HTTP 応答の最大数

ルータにバッファされる、URL フィルタ サーバからの HTTP レスポンスの数を設定できます。この数値に到達すると、ルータではそれ以上のレスポンスが破棄されます。デフォルト値は 200 です。0 ～ 20000 の値を設定できます。

詳細

［詳細］ボックスでは、送信元インターフェイスを選択できます。［送信元インターフェイス］リストからインターフェイスを選択します。

ローカル URL リスト

ルータ上の Cisco IOS イメージで、URL フィルタリングがサポートされ、ゾーンベースのポリシー ファイアウォール（ZPF）はサポートされない場合、ルータ上では 1 つのローカル URL リストを管理できます。このリストは、URL フィルタリングを有効にするすべてのアプリケーション セキュリティ ポリシーにより使用されます。12.4(9)T 以降の Cisco IOS イメージは、Cisco CP でサポートされるすべての ZPF 機能に対応しています。ZPF 設定では、URL フィルタリングのパラメータ マップごとにローカル URL リストを作成できます。

Cisco CP を使用してリスト エントリを作成することも、PC に保存されたリストからエントリをインポートすることもできます。ローカル URL リストと URL フィルタ サーバとを組み合せて使用する場合は、ローカルのエントリが最初に使用されます。詳細については、「URL フィルタリングの優先順位」を参照してください。

ローカル URL リストの管理

Cisco CP を使用してローカル URL リストを管理するときには、エントリを 1 つずつ追加 / 削除することも、PC から URL リストをインポートしてから Cisco CP による各エントリの処理方法を指定することもできます。ルータ上のリストの特定エントリを管理するには、［追加］ボタン、および［削除］ボタンを使用します。PC から URL リストをインポートするには、［URL リストのインポート］をクリックします。

（注）　ローカル リストからエントリを削除する場合、ルータが URL フィルタ サーバを使用するように設定されていると、ローカル リストから削除するエントリと一致するエントリが、それらのサーバ上にも存在する可能性があります。

ルータ上の全エントリを削除するには、［すべて削除］ボタンを使用します。ローカル リストがルータ上に設定されていない場合には、設定された URL フィルタ サーバがルータで使用されます。削除する URL リストを後で取得したい場合には、すべてのエントリを削除する前に［URL リストのエクスポート］ボタンを使用して、URL リストを PC に保存します。URL リストを PC に保存すると、リストには拡張子 .CSV が付加されます。

PC からの URL リストのインポート

URL リストを PC からルータにインポートするには、[URL リストのインポート] ボタンを使用します。拡張子 .txt または .CSV の URL リストを選択する必要があります。PC でリストを選択すると、リストの各エントリに対する処理を指定できるダイアログが Cisco CP に表示されます。詳細については、「URL リストのインポート」を参照してください。

ローカル URL の追加または編集

このウィンドウでは、ルータのローカル URL リストの URL エントリを追加または編集できます。フル ドメイン名または部分ドメイン名を入力し、この URL に対する要求を**許可**するか、**拒否**するかを選択します。

フル ドメイン名（www.somedomain.com など）を入力した場合、このドメイン名を含むすべての要求（www.somedomain.com/news や www.somedomain.com/index など）が、このダイアログで選択した設定に基づいて許可または拒否されます。これらの要求は、ルータで使用するよう設定されている URL フィルタ サーバには送信されません。

部分ドメイン名（.somedomain.com など）を入力した場合、この文字列で終了するすべての要求（www.somedomain.com/products や wwwin/somedomain.com/eng など）が、このダイアログで選択した設定に基づいて許可または拒否されます。これらの要求は、ルータで使用するよう設定されている URL フィルタ サーバには送信されません。

URL リストのインポート

このダイアログ ボックスでは、PC からルータにインポートする URL リストを確認して、各エントリに対する処理を指定することができます。このダイアログにある URL エントリがまだルータ上にない場合には、[追加] をクリックしてルータのリストに追加できます。URL エントリがすでにルータ上に存在し、このダイアログにあるエントリで置き換える場合には、[置換] をクリックします。

デフォルトでは、[インポート] カラムのすべてのボックスが選択されています。ルータに送信しないエントリがある場合は、それらエントリの横のボックスの選択を解除します。すべてのボックスの選択を解除する場合には、[すべての選択を解除] をクリックします。[すべて選択] をクリックすると、すべてのボックスが選択されます。

[追加] をクリックすると、選択した URL エントリがまだ URL リストになければ、リストに追加されます。すでに URL リストにあるエントリを追加しようとした場合は、エントリのドメインに指定されたアクションがリストにすでに存在するアクションと異なっていても、エントリが追加されません。

ルータ上の URL リストにすでに存在するエントリに対して異なるアクションを指定するには、[置換] ボタンを使用します。選択したエントリがルータ上のリストにない場合には、[置換] を使用しても何も行われません。

URL フィルタ サーバ

ルータからは HTTP リクエストを URL フィルタ サーバに送信できます。サーバでは、ルータで保存できるよりもはるかに多くの URL リストを保存できます。ルータが URL フィルタ サーバ リストを使用するように設定されている場合、ルータは、ローカル リストのエントリに一致しない要求を、接続している URL フィルタ サーバに送信し、サーバから受信した応答に基づいて要求を許可または拒否します。ルータが接続しているサーバが停止した場合、ルータは、接続が確立されるまでリスト内のサーバに順にアクセスします。

URL フィルタ サーバのリストは、ローカル URL リストと共に使用できます。ルータによるこれら両方のリソースの使用方法については、「URL フィルタリングの優先順位」を参照してください。

[追加] をクリックし、[Secure Computing] または [Websense] を選択して、追加するサーバのタイプを指定します。

（注）　Cisco IOS ソフトウェアで使用できるのは 1 つのタイプの URL フィルタ サーバのみであり、異なるタイプのサーバをリストに追加することはできません。たとえば、Websense サーバを含む URL フィルタ サーバ リストがルータに設定されている場合に、Secure Computing サーバをリストに追加しようとすると、エラー メッセージが通知されます。URL フィルタ サーバ リストに現在、1 タイプのサーバが含まれており、これを別のタイプに変更する場合には、リストのすべてのサーバ エントリを削除してから、新しいタイプのエントリを追加しなければなりません。

このウィンドウにはリストの各 URL フィルタ サーバの設定が表示されます。各設定値の説明については、「URL フィルタ サーバの追加 / 編集」を参照してください。

URL フィルタ サーバの追加 / 編集

Websense または Secure Computing URL フィルタ サーバの情報を指定します。

IP アドレス / ホスト名

サーバの IP アドレスまたはホスト名を入力します。ホスト名を入力する場合、ルータは、ホスト名を IP アドレスに解決できるように、DNS サーバに接続していなければなりません。

方向

URL フィルタ サーバが内部ネットワークの一部である場合は、［内部］を選択します。これは通常、ルータ LAN インターフェイスが接続するネットワークの 1 つです。ルータが外部ネットワークにある場合には、［外部］を選択します。これは通常、ルータ WAN インターフェイスが接続するネットワークの 1 つです。デフォルト値は［内部］です。

ポート番号

追加する URL フィルタ サーバのタイプのデフォルト ポート番号が自動的に設定されます。Websense サーバを追加する場合、デフォルト値は 15868 です。Secure Computing サーバを追加する場合、デフォルト値は 4005 です。番号がデフォルト値と異なる場合は、サーバがリッスンするポートの番号に変更します。このフィールドには 1 ～ 65535 の値を指定できます。

再送信カウント

オプション フィールド。サーバからの応答がない場合にルータで要求の再送信が試行される回数を入力します。デフォルト値は 2 回です。このフィールドには 1 ～ 10 の値を指定できます。

再送信のタイムアウト

オプション フィールド。ルータが要求を再送信する前にサーバからの応答を待つ時間（秒単位）を入力します。デフォルト値は 5 秒です。

URL フィルタリングの優先順位

［設定］>［セキュリティ］>［ファイアウォールと ACL］>［アプリケーション セキュリティ］>［URL フィルタリング］と進み、［URL フィルタリングの有効化］をクリックして、URL フィルタリングを有効にする必要があります。これを実行できるのは、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る場合だけです。

URL フィルタリングが有効になっていると、ルータで、次のように HTTP リクエストの処理方法が決定されます。

- HTTP リクエストの URL が、ルータ上のローカル URL リストのエントリに一致した場合は、そのエントリに基づいてリクエストが許可または拒否されます。
- HTTP リクエストの URL が、ローカル URL リストのエントリに一致しない場合は、接続している URL フィルタ サーバにそのリクエストが送信されます。そのサーバから返される情報に基づいて、リクエストが許可または拒否されます。

- 許可モードが無効になっていて、ルータが URL フィルタ サーバとの接続を確立できない場合、リクエストは拒否されます。デフォルトでは、許可モードは無効に設定されています。
- 許可モードが有効で、ルータが URL フィルタ サーバとの接続を確立できない場合、リクエストは許可されます。許可モードは、［グローバル設定の編集］ダイアログで有効にします。

ルータ上に設定できるのは、URL リスト 1 つおよび URL フィルタ サーバ リスト 1 つだけです。設定されているすべてのアプリケーション セキュリティ ポリシーでは、同じ URL リストと URL フィルタ サーバ リストが使用されます。これらのリストは、［アプリケーション セキュリティ］ウィンドウか、［追加タスク］>［URL フィルタリング］から管理できます。すべてのアプリケーション セキュリティ ポリシーが削除された場合でも、URL リストと URL フィルタ サーバ リストは［追加タスク］ウィンドウで管理できます。ただし、アプリケーション セキュリティ ポリシーで URL フィルタリングが有効になっていないと、ルータで URL フィルタリングが実行されません。