CHAPTER 19

トラフィックのフィルタリング

ここでは、次の項目について説明します。

Filter Rules

Filter Rules ウィンドウには設定済みのフィルタ ルールが表示され、新しいフィルタ ルールを追加、または既存のルールを変更するためのオプションが提供されます。フィルタ ルールでは、適用するフィルタリングのタイプと、適用先となるトラフィックの種類が指定されます。

（注） HTTP、HTTPS、または FTP フィルタ ルールを追加する前に、URL フィルタリング サーバをイネーブルにする必要があります。URL フィルタリング サーバをイネーブルにするには、**Features** > **Configuration** > **Properties** > **URL Filtering** 画面を使用します。詳細については、「URL Filtering」を参照してください。

利点

Filter Rules ウィンドウでは、現在 FWSM 上に設定されているフィルタ ルールについての情報が提供されます。また、フィルタ ルールを追加または変更し、ウィンドウに表示される詳細の量の増減に使用できるボタンも提供されます。

フィルタリングにより、セキュリティ ポリシーで FWSM の通過を許可するトラフィックを自在に制御できます。アクセスを全面的にブロックする代わりに、ActiveX オブジェクトや Java アプレットなど、特定の状況でセキュリティ上の脅威をもたらす可能性のある特定の不適切なオブジェクトを HTTP トラフィックから取り除くことができます。また、URL フィルタリングを使用して、**Secure Computing SmartFilter** や Websense などの外部フィルタリング サーバに特定のトラフィックを誘導することもできます。これらのサーバは、セキュリティ ポリシーで指定されている特定のサイトまたは特定のタイプのサイトに向かうトラフィックをブロックできます。

URL フィルタリングは CPU に大きな負荷がかかるため、外部フィルタリング サーバを使用することにより、他のトラフィックのスループットに影響を与えることがなくなります。ただし、ネットワークの速度および URL フィルタリング サーバのキャパシティによっては、フィルタ対象のトラフィックの最初の接続に必要な時間が著しく長くなる場合もあります。

フィールド

- **No**：ルールの数値識別子。数値の順序でルールが適用されます。
- **Source**：フィルタリング アクションが適用されるソース ホストまたはネットワーク。
- **Destination**：フィルタリング アクションが適用される宛先ホストまたはネットワーク。
- **Service**：フィルタリング アクションが適用されるプロトコルまたはサービスを指定します。
- **Action**：適用するフィルタリング アクションのタイプ。
- **Options**：特定のアクションに対してイネーブルになっているオプションを示します。
- **Add**：追加できるフィルタ ルールのタイプが表示されます。ルールの種類をクリックすると、指定したフィルタ ルールのタイプの **Add Filter Rule** ダイアログボックスが開きます。
  - Add Filter ActiveX Rule
  - Add Filter Java Rule
  - Add Filter HTTP Rule
  - Add Filter HTTPS Rule
  - Add Filter FTP Rule
- **Edit**：選択したフィルタリング ルールを編集するための **Edit Filter Rule** ダイアログボックスを表示します。
- **Delete**：選択したフィルタリング ルールを削除します。
- Cut：フィルタ ルールを切り取って別の場所に配置します。
- Copy：フィルタ ルールをコピーできます。
- Paste：フィルタ ルールを別の場所に貼り付けます。
- Find：フィルタ ルールを検索します。このボタンをクリックすると、拡張ツールバーが表示されます。
  - Filter：ドロップダウン メニューを使用して、送信元、宛先、ソース、アクション、またはルール クエリーで検索できます。
  - ....：フィルタのソースを選択し、Select Source ダイアログボックスが表示されます。
  - Filter：フィルタを入力します。
  - Clear：フィルタ ルールをクリアします。
  - Rule Query：ルールを検索するクエリーを作成します。
- Rule Diagram：Rule Diagram の表示を切り替えます。
- 選択しているフィルタ ルールのソースを選ぶには、Addresses タブを使用します。
  - Type：ドロップダウン メニューからソースを選択します。All、IP Address Objects、IP Names、または Network Object の各グループから選択します。
  - Name：フィルタ ルール名を一覧表示します。
  - Add：フィルタ ルールを追加します。
  - Edit：フィルタ ルールを編集します。
  - Delete：フィルタ ルールを削除します。
  - Find：フィルタ ルールを検索します。
- 事前定義済みフィルタ ルールを選択するには、Services タブを使用します。
  - Type：ドロップダウン メニューからソースを選択します。All、IP Address Objects、IP Names、または Network Object の各グループから選択します。
  - Name：フィルタ ルール名を一覧表示します。
  - Edit：フィルタ ルールを編集します。
  - Delete：フィルタ ルールを削除します。
  - Find：フィルタ ルールを検索します。

- フィルタ ルールの時間範囲を選択するには、Time Ranges を使用します。
  - Add：フィルタ ルールの時間範囲を追加します。
  - Edit：フィルタ ルールの時間範囲を編集します。
  - Delete：フィルタ ルールの時間範囲を削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Filter Rule

ルールを適用するインターフェイスの指定、ルールを適用するトラフィックの指定、または特定タイプのフィルタリング アクションの設定には、Add Filter Rule ダイアログボックスを使用します。

（注）　HTTP、HTTPS、または FTP フィルタ ルールを追加する前に、URL フィルタリング サーバをイネーブルにする必要があります。URL フィルタリング サーバをイネーブルにするには、**Configuration** > **Properties** > **URL Filtering** 画面を使用します。詳細については、「URL Filtering」を参照してください。

フィールド

- **Action**：適用するさまざまなフィルタリング アクションに関して、次に挙げるリストを提供します。
  - Filter ActiveX
  - Do not filter ActiveX
  - Filter Java
  - Do not filter Java
  - Filter HTTP (URL)
  - Do not filter HTTP (URL)
  - Filter HTTPS
  - Do not filter HTTPS
  - Filter FTP

- Do not filter FTP

Rule Flow Diagram and the Filtering Option グループ ボックスは、選択するフィルタリング アクションによって変わります。

- Source Host/Network
  - IP Address：フィルタリング アクションの適用先であるトラフィックを指定する IP アドレスを使用します。
  - Name：フィルタリング　アクションの適用先であるトラフィックを指定する名前を使用します。
  - Name : Name ボタンが選択されているとき、フィルタリング アクションの適用先であるトラフィックの指定に使用される名前を指定します。
  - Interface：フィルタリング アクションの適用先であるインターフェイスを指定します。
  - IP Address：IP アドレスの選択時にフィルタリング アクションの適用先であるトラフィックの指定に使用される IP アドレスを指定します。
  - Mask：IP Address が選択されているとき、フィルタリング アクションの適用先であるトラフィックの指定に使用されるサブネット マスクを指定します。
- Destination Host/Network
  - IP Address：フィルタリング アクションの適用先であるトラフィックを指定します。
  - Name：フィルタリング アクションの適用先であるトラフィックを示します。
  - Name：Name　が選択されているとき、フィルタリング　アクションの適用先であるトラフィックの指定に使用される名前を指定します。
  - Interface：フィルタリング アクションの適用先であるインターフェイスを指定します。
  - IP Address：IP アドレスの選択時にフィルタリング アクションの適用先であるトラフィックの指定に使用される IP アドレスを指定します。
  - Mask：IP Address が選択されているとき、フィルタリング アクションの適用先であるトラフィックの指定に使用されるサブネット マスクを指定します。
- Browse : Select host/network ダイアログボックスが表示されます。このダイアログボックスでは、事前に設定されたリストからホストまたはネットワークを選択できます。
- Rule Flow Diagram : FWSM を介して転送されるトラフィックに特定のフィルタリング アクションが適用される仕組みをグラフィカルな表現で示します。
- HTTP Filtering Option：このグループ ボックスは、ドロップダウン リストで Filter HTTP オプションを選択したときにのみ表示されます。
  - Filter HTTP on port(s) : FWSM がフィルタリング アクションの適用先であるトラフィックをリッスンする TCP/UDP ポートを指定します。
  - Block connections to proxy server：プロキシ サーバを介した HTTP 要求を禁止します。
  - Allow outbound traffic if URL server is not available : イネーブルになっているとき、URL フィルタリング サーバがダウンしたり、FWSM への接続が中断されたりする場合、ユーザは URL フィルタリングが実行されない状態で接続できます。このオプションがディセーブルになっている場合、URL サーバが使用不能になると、ユーザはインターネット Web サイトに接続できません。
  - Truncate CGI requests by removing the CGI parameters：FWSM は、パラメータなしの CGI スクリプトの場所とスクリプト名だけをフィルタリング サーバに転送します。
- Long URL：このグループ ボックスは、ドロップダウン リストで Filter HTTP オプションを選択したときにのみ表示されます。

  FWSM では、最大 1159 バイトの URL をフィルタリングできます。Websense フィルタリング サーバを使用する場合、フィルタリング可能な URL は最大 4 KB です。長い URL のフィルタリングをイネーブルにするには、**Configuration** > **Properties** > **URL Filtering** > **Advanced** 画面を使用します。詳細については、「URL Filtering」を参照してください。
  - Drop : FWSM は最大値よりも長い URL をドロップし、ユーザはターゲットのインターネット Web サイトに接続できません。

  - Truncate：FWSM は URL を許可されている最大の長さに短縮し、短縮後の URL を分析のためにフィルタリング サーバに転送します。
  - Block：許可されている最大値よりも長い URL にユーザが接続できないようにします。
- HTTPS Filtering Option：このグループ ボックスは、ドロップダウン リストで Filter HTTPS オプションを選択したときにのみ表示されます。
  - Filter HTTPS on port(s)：FWSM がフィルタリング アクションの適用先であるトラフィックをリッスンする TCP/UDP ポートを指定します。
  - Allow outbound traffic if URL server is not available：イネーブルになっているとき、URL フィルタリング サーバがダウンしたり、FWSM への接続が中断されたりする場合、ユーザは URL フィルタリングが実行されない状態で接続できます。このオプションがディセーブルになっている場合、URL サーバが使用不能になると、ユーザはインターネット Web サイトに接続できません。

- FTP Filtering Option：このグループ ボックスは、ドロップダウン リストで Filter FTP オプションを選択したときにのみ表示されます。
  - Filter FTP on port(s)：FWSM がフィルタリング アクションの適用先であるトラフィックをリッスンする TCP/UDP ポートを指定します。
  - Allow outbound traffic if URL server is not available：イネーブルになっているとき、URL フィルタリング サーバがダウンしたり、FWSM への接続が中断されたりする場合、ユーザは URL フィルタリングが実行されない状態で接続できます。このオプションがディセーブルになっている場合、URL サーバが使用不能になると、ユーザはインターネット Web サイトに接続できません。
  - Block outbound traffic if absolute FTP path is not provided：イネーブルになっているとき、FTP ディレクトリへの相対パス名を使用している場合は、FTP 要求がドロップされます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

- Filter Rules
- URL Filtering

URL Filtering

フィルタリングは、セキュリティの高いネットワークからセキュリティの低いネットワークに発信される接続要求に対して適用できます。ACL を使用して特定のコンテンツ サーバに対する発信アクセスを禁止することはできますが、サイズおよびインターネットのダイナミックな性質により、このような手段で使用方法を管理することは困難です。次のインターネット フィルタリング製品のいずれかを実行する別個のサーバを使用することにより、コンフィギュレーションを簡素化し、FWSM のパフォーマンスを向上できます。

- HTTP、HTTPS、および FTP フィルタリング用の Websense Enterprise
- HTTP のフィルタリング専用の **Secure Computing SmartFilter**（Sentian の一部のバージョンでは HTTPS をサポートしていますが、FWSM では、Sentian での HTTP のフィルタリングのみをサポートしています。）

FWSM のパフォーマンスへの影響は、外部サーバを使用した方が小さくなりますが、フィルタリング サーバが FWSM から離れている場合は、Web サイトまたは FTP サーバへのアクセス時間が長くなることもあります。

フィルタリングがイネーブルで、コンテンツを求める要求が FWSM を経由して送信された場合、その要求はコンテンツ サーバとフィルタリング サーバに同時に送信されます。フィルタリング サーバがその接続を許可した場合、FWSM はコンテンツ サーバからの応答を発信元クライアントに転送します。フィルタリング サーバがその接続を拒否した場合、FWSM は応答をドロップし、接続が成功しなかったことを示すメッセージまたはリターン コードを送信します。

FWSM 上でユーザ認証がイネーブルの場合、FWSM はフィルタリング サーバにユーザ名も送信します。フィルタリング サーバは、ユーザ固有のフィルタリング設定を使用したり、使用方法に関する高度なレポートを提供したりすることができます。

一般的な手順

次に、外部フィルタリング サーバを使用するフィルタリングをイネーブルにする手順をまとめます。

ステップ 1　フィルタリング サーバを指定します。

ステップ 2　（オプション）コンテンツ サーバからの応答をバッファに格納します。

ステップ 3　（オプション）コンテンツ サーバのアドレスをキャッシュしてパフォーマンスを向上させます。

ステップ 4　フィルタリング ルールを設定します。「**Filter Rules**」を参照してください。

ステップ 5　外部フィルタリング サーバを設定します。詳細については、次の Web サイトを参照してください。

- http://www.websense.com
- http://www.securecomputing.com

コンテキストごとに最大 4 つのフィルタリング サーバを指定できます。シングルモードでは、最大 16 個のサーバを指定できます。FWSM は、1 つのサーバが応答するまで、それらのサーバを順番に使用します。コンフィギュレーション内に設定できるサーバのタイプは、1 つだけ（Websense または Secure Computing SmartFilter）です。

（注）　HTTP、HTTPS、または FTP フィルタリング ルールのフィルタリングを設定する前に、フィルタリング サーバを追加する必要があります。

フィールド

- **URL Filtering Server** 領域
  - **Websense**：Websense URL フィルタリング サーバをイネーブルにします。
  - **Secure Computing SmartFilter**：Secure Computing SmartFilter URL フィルタリング サーバをイネーブルにします。
  - **Secure Computing SmartFilter Port**：**Secure Computing SmartFilter** ポートを指定します。デフォルトは 4005 です。
  - **Interface**：フィルタリング サーバに接続しているインターフェイスを表示します。
  - **IP Address**：フィルタリング サーバの IP アドレスを表示します。
  - **Timeout**：フィルタリング サーバへの要求がタイムアウトになってからの秒数を表示します。
  - **Protocol**：フィルタリング サーバとの通信に使用されるプロトコルを表示します。
  - **TCP Connections**：URL フィルタリング サーバと通信できる TCP 接続の最大数を表示します。
  - **Add**：Websense または **Secure Computing SmartFilter** を選択したかどうかにより、新しいフィルタリング サーバを追加します。
  - **Insert**：現在選択しているサーバより優先順位の高い位置に新しいフィルタリング サーバを追加します。
  - **Edit**：選択したフィルタリング サーバのパラメータを変更できます。
  - **Delete**：選択したフィルタリング サーバを削除します。
- **Apply**：実行中のコンフィギュレーションに変更を適用します。
- **Reset**：まだ適用されていない変更を削除します。
- **Advanced**：バッファリング キャッシング、長い URL のサポートなど、高度なフィルタリング パラメータを表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

Filter Rules

Add/Edit Parameters for Websense URL Filtering

- **Interface**：URL フィルタリング サーバの接続を行うインターフェイスを指定します。
- **IP Address**：URL フィルタリング サーバの IP アドレスを指定します。
- **Timeout**：フィルタリング サーバへの要求がタイムアウトになってからの秒数を指定します。
- **Protocol** 領域
  - **TCP 1**：Websense URL フィルタリング サーバとの通信に TCP バージョン 1 を使用します。
  - **TCP 4**：Websense URL フィルタリング サーバとの通信に TCP バージョン 4 を使用します。
  - **UDP 4**：Websense URL フィルタリング サーバとの通信に UDP バージョン 4 を使用します。
- **TCP Connections**：URL フィルタリング サーバと通信できる TCP 接続の最大数を指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Parameters for Secure Computing SmartFilter URL Filtering

- **Interface**：URL フィルタリング サーバの接続を行うインターフェイスを指定します。
- **IP Address**：URL フィルタリング サーバの IP アドレスを指定します。
- **Timeout**：フィルタリング サーバへの要求がタイムアウトになってからの秒数を指定します。
- **Protocol** 領域
  - **TCP**：**Secure Computing SmartFilter** URL フィルタリング サーバとの通信に TCP を使用します。
  - **UDP**：**Secure Computing SmartFilter** URL フィルタリング サーバとの通信に UDP を使用します。

TCP Connections：URL フィルタリング サーバと通信できる TCP 接続の最大数を指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Advanced URL Filtering

フィールド

URL Cache Size 領域

ユーザがサイトにアクセスすると、フィルタリング サーバは FWSM に対して、サーバ アドレスを一定時間キャッシュすることを許可できます。ただし、そのアドレスでホストされているサイトはいずれも、常に許可されるカテゴリに属している必要があります。これによって、そのユーザがそのサーバに再度アクセスするか、別のユーザがそのサーバにアクセスしたときに、FWSM がフィルタリング サーバに再度照会する必要がなくなります。

（注）　キャッシュされた IP アドレス要求は、フィルタリング サーバに渡されず、記録もされません。そのため、このアクティビティはどのレポートにも表示されません。

- **Enable caching based on**：指定した基準に基づいて、キャッシングをイネーブルにします。
  - **Destination Address**：URL 宛先アドレスに基づいてエントリをキャッシュします。このモードは、すべてのユーザが Websense サーバ上で同一の URL フィルタリング ポリシーを共有している場合に選択します。
  - **Source/Destination Address**：URL 要求を開始した送信元アドレスと、URL 宛先アドレスの両方に基づいてエントリをキャッシュします。このモードは、ユーザがサーバ上で同じ URL フィルタリング ポリシーを共有していない場合に選択します。
- **Cache size**：キャッシュのサイズを指定します。

URL Buffer Size 領域

ユーザがコンテンツ サーバへの接続要求を発行した場合、その要求は、FWSM によって、コンテンツ サーバとフィルタリング サーバの両方に同時に送信されます。フィルタリング サーバがコンテンツ サーバより早く応答しなかった場合、サーバ応答はドロップされます。これによって、Web クライアント側の視点で Web サーバ応答が表示されます。これは、クライアントが要求を再発行する必要があるためです。

HTTP 応答バッファをイネーブルにすると、Web コンテンツ サーバからの応答はバッファリングされ、フィルタリング サーバによって接続が許可された場合に、要求クライアントに転送されます。これによって、バッファリングしない場合に発生する可能性のある遅延が回避されます。

- **Enable buffering**：要求のバッファリングをイネーブルにします。
  - **Number of 1550-byte buffers**：1550 バイト バッファの数を指定します。

Long URL Support 領域

デフォルトでは、FWSM は、1159 文字を超える HTTP URL を長い URL と見なします。Websense サーバの場合、最大許容長を増やすことができます。

- **Use Long URL**：Websense フィルタリング サーバの長い URL をイネーブルにします。
- **Maximum Long URL Size**：URL の最大許容長を 4 KB を上限として指定します。
- **Memory Allocated for Long URL**：長い URL に割り当てるメモリを指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—