CHAPTER 22

フィルタ ルールの設定

ここでは、次の項目について説明します。

- URL フィルタリング（P. 22-1）
- Filter Rules（P. 22-6）

URL フィルタリング

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、セキュリティ アプライアンス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、セキュリティ アプライアンスでは、Sentian での HTTP のフィルタリングのみをサポートしています）

セキュリティ アプライアンス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 サーバがセキュリティ アプライアンス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セキュリティ アプライアンス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、セキュリティ アプライアンスはコンテンツ 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、セキュリティ アプライアンス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。

セキュリティ アプライアンス上でユーザ認証がイネーブルの場合、セキュリティ アプライアンスはフィルタリング 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。

ここでは、次の項目について説明します。

- URL フィルタリングの設定（P. 22-2）
- URL Filtering Servers（P. 22-2）
- Advanced URL Filtering（P. 22-4）

URL フィルタリングの設定

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　**Configuration > Firewall > URL Filter Servers** に移動し、外部フィルタリング サーバを指定します。P.22-2 の「URL Filtering Servers」を参照してください。

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。P.22-4 の「Advanced URL Filtering」を参照してください。

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。P.22-4 の「Advanced URL Filtering」を参照してください。

ステップ 4　**Configuration > Firewall > Filter Rules** に移動し、フィルタ ルールを設定します。P.22-6 の「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

URL Filtering Servers

URL Filtering Servers ペインでは、使用する外部フィルタ サーバを指定できます。コンテキストごとに最大 4 つの同じタイプのフィルタリング サーバを指定できます。シングルモードでは、最大 16 台の同じタイプのフィルタリング サーバが許容されます。セキュリティ アプライアンスは、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 Type 領域には次のフィールドがあります。

- 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。

URL Filtering Servers 領域には次のフィールドがあります。

- 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。詳細については、次の項目を参照してください。
  - Add/Edit Parameters for Websense URL Filtering（P. 22-3）
  - Add/Edit Parameters for Secure Computing SmartFilter URL Filtering（P. 22-4）
- Insert Before：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。
- Insert After：現在選択しているサーバより優先順位の低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。

このペインで次のアクションを実行できます。

- 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

Advanced URL Filtering（P. 22-4）

Filter Rules（P. 22-6）

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 サーバはセキュリティ アプライアンスに対して、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、セキュリティ アプライアンスがフィルタリング 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、セキュリティ アプライアンスによって、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。1 ～ 128 の範囲の値を指定できます。
- Long URL Support 領域

  デフォルトでは、セキュリティ アプライアンスは、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
•	•	•	•	—

Filter Rules

Filter Rules ペイン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、**Configuration > Firewall > URL Filtering Servers** ペインを使用します。詳細については、P.22-1 の「URL フィルタリング」を参照してください。

利点

Filter Rules ウィンドウでは、現在セキュリティ アプライアンス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 ポリシーでセキュリティ アプライアンス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 ルールを表示します。ルール タイプをクリックすると、指定したフィルタ ルール タイプに対する次の 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。詳細については、P.22-9 の「ルール テーブルのフィルタリング」を参照してください。
- Rule Diagram：Rule Diagram の表示を切り替えます。
- Packet Trace：Packet Tracer ユーティリティを起動します。
- 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できます。All、IP Address Objects、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できます。All、IP Address Objects、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
•	•	•	•	—

フィルタ ルールの追加および編集

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、**Features** > **Configuration** > **Properties** > **URL Filtering** 画面を使用します。詳細については、「URL フィルタリング」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 アクションに対して、次に挙げるドロップダウン リストを提供します（表示されるアクションは、作成中または編集中のフィルタ ルールのタイプに応じて異なります）。
  - Filter ActiveX
  - Do not filter ActiveX
  - Filter Java Applet
  - Do not filter Java Applet
  - Filter HTTP (URL)
  - Do not filter HTTP (URL)
  - Filter HTTPS
  - Do not filter HTTPS
  - Filter FTP
  - Do not filter FTP
- Source：フィルタリング アクションが適用されるトラフィックの送信元を指定します。送信元は次のいずれかの方法で入力できます。
  - any：任意の送信元アドレスを指定するには、「any」（かぎカッコなし）と入力します。
  - *name*：ホスト名を入力します。
  - *address*/*mask*：IP アドレスと、オプションでネットワーク マスクを入力します。ネットマスクの表現は、CIDR またはドット付き 10 進数表記のいずれでも可能です。たとえば、10.1.1.0/24 または 10.1.1.0/255.255.255.0 と入力できます。
  - ...：Browse Source ダイアログボックスを開きます。リストからホストまたはアドレスを選択できます。
- Destination：フィルタリング アクションが適用されるトラフィックの宛先を指定します。宛先は次のいずれかの方法で入力できます。
  - any：任意の宛先アドレスを指定するには、「any」（かぎカッコなし）と入力します。
  - *name*：ホスト名を入力します。
  - *address*/*mask*：IP アドレスと、オプションでネットワーク マスクを入力します。ネットマスクの表現は、CIDR またはドット付き 10 進数表記のいずれでも可能です。たとえば、10.1.1.0/24 または 10.1.1.0/255.255.255.0 と入力できます。
  - ...：Browse Destination ダイアログボックスを開きます。リストからホストまたはアドレスを選択できます。
- Service：フィルタリング アクションが適用されるトラフィックのサービスを指定します。宛先は次のいずれかの方法で入力できます。
  - tcp/*port*：1 ～ 65535 のポート番号を指定できます。さらに、TCP サービスには次の修飾子を使用できます。

    !=：～と等しくない。たとえば、!=tcp/443 と指定します。

    <：～より小さい。たとえば、<tcp/2000 と指定します。

    >：～より大きい。たとえば、>tcp/2000 と指定します。

    -：範囲。たとえば、tcp/2000-3000 と指定します。
  - *name*：ウェルノウン サービス名（http や ftp など）を入力します。
  - ...：Browse Service ダイアログボックスを開きます。サービスをリストから選択できます。
- HTTP Options：この領域は HTTP フィルタ ルールの場合だけ表示されます。
  - When URL exceeds maximum permitted size：URL が指定されたサイズを超えた場合に実行するアクションを選択します。URL の切り捨て、またはトラフィックのブロックを選択できます。

  - 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、セキュリティ アプライアンス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の場合、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 users from connecting to an HTTP proxy server：プロキシ サーバを介した HTTP 要求を禁止します。
  - Truncate CGI parameters from URL sent to URL server：セキュリティ アプライアンスは、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。
- HTTPS Options：この領域は、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。
  - 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、セキュリティ アプライアンス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の場合、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 Options：この領域は、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。
  - 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、セキュリティ アプライアンス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の場合、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 interactive FTP sessions (block 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
•	•	•	•	—

ルール テーブルのフィルタリング

ルール テーブルに大量のエントリがあると、特定のルールを見つけにくい場合があります。ルール テーブルにフィルタを適用し、フィルタで指定されたルールだけを表示させることができます。ルール テーブルをフィルタリングするには、次の手順を実行します。

ステップ 1　ツールバーで **Find** をクリックします。Filter ツールバーが表示されます。

ステップ 2　フィルタ リストから次のようにフィルタのタイプを選択します。

- Source：指定した送信元アドレスまたはホスト名に基づいてルールを表示します。
- Destination：指定した宛先アドレスまたはホスト名に基づいてルールを表示します。
- Source or Destination：指定した送信元または宛先のアドレスまたはホスト名に基づいてルールを表示します。

- Service：指定したサービスに基づいてルールを表示します。
- Rule Type：指定したルール タイプに基づいてルールを表示します。
- Query：送信元、宛先、サービス、およびルール タイプ情報で構成される複合クエリーに基づいてルールを表示します。

ステップ 3　Source、Destination、Source or Destination、および Service がフィルタの場合は、次の手順を実行します。

a. リストから照合基準を選択します。文字列を完全一致させるには「is」（かぎカッコなし）、部分一致させるには「contains」を選択します。

b. 照合する文字列を次のいずれかの方法で入力します。

- Condition フィールドに、送信元、宛先、またはサービスの名前を入力します。
- **...** をクリックすると参照ダイアログが開き、そこから既存のサービス、IP アドレス、またはホスト名を選択できます。

ステップ 4　Rule Type フィルタの場合は、リストからルール タイプを選択します。

ステップ 5　Query フィルタの場合は、**Define Query** をクリックし、複合クエリーを設定します。複合クエリーの設定の詳細については、P.22-11 の「Browse Source/Destination/Service」を参照してください。

ステップ 6　ルール テーブルにフィルタを適用するには、**Filter** をクリックします。

ステップ 7　ルール テーブルからフィルタをクリアしてすべてのルール エントリを表示するには、**Clear** をクリックします。

Define Query

Define Query ダイアログボックスでは、送信元、宛先、サービス、ルール タイプなど、複数の基準に基づいてルール テーブル フィルタを定義できます。

クエリーを作成したら、OK をクリックします。フィルタがただちにルール テーブルに適用されます。Clear をクリックすると、フィルタをクリアできます。

フィールド

- Source：送信元の IP アドレスまたはホスト名。完全一致には「is」、部分一致には「contains」を選択します。**...** をクリックすると選択ダイアログが開きます。CIDR 表記（アドレス / ビットカウント）を使用してネットワーク マスクを指定できます。複数のアドレスは、カンマ（,）で区切って指定できます。
- Destination：宛先の IP アドレスまたはホスト名。完全一致には「is」、部分一致には「contains」を選択します。**...** をクリックすると選択ダイアログが開きます。CIDR 表記（アドレス / ビットカウント）を使用してネットワーク マスクを指定できます。複数のアドレスは、カンマ（,）で区切って指定できます。
- Source or Destination：送信元または宛先の IP アドレスまたはホスト名。完全一致には「is」、部分一致には「contains」を選択します。**...** をクリックすると選択ダイアログが開きます。CIDR 表記（アドレス / ビットカウント）を使用してネットワーク マスクを指定できます。複数のアドレスは、カンマ（,）で区切って指定できます。
- サービス：サービスのプロトコル / ポートまたは名前。　完全一致には「is」、部分一致には「contains」を選択します。**...** をクリックすると選択ダイアログが開きます。複数のサービスは、カンマ（,）で区切って指定できます。
- Rule Type：リストからルール タイプを選択します。

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

ルール テーブルのフィルタリング（P. 22-9）

Browse Source/Destination/Service

Browse Source/Destination/Service ダイアログボックスでは、既存の IP アドレス オブジェクト、名前オブジェクト、またはサービス オブジェクトから選択できます。

フィールド

- Add：新しい IP アドレス オブジェクト、名前オブジェクト、またはサービス オブジェクトを追加します。
- Edit：既存の IP アドレス オブジェクト、名前オブジェクト、またはサービス オブジェクトを編集します。
- Filter/Clear：ダイアログボックスに表示されている情報をフィルタリングするための文字列を入力します。ダイアログボックスに表示されている情報にフィルタを適用するには、**Filter** をクリックします。フィルタを削除し、すべてのオブジェクトを表示するには、**Clear** をクリックします。
- Type：表示されているオブジェクトをタイプ（IP アドレス オブジェクトなど）別に整理します。
- Name：オブジェクトの名前。サービスの場合はサービス名です。IP アドレス オブジェクトの場合は IP アドレス、IP 名オブジェクトの場合はホスト名です。
- IP Address：アドレス オブジェクトの IP アドレス。
- Netmask：アドレス オブジェクトのネットワーク マスク。
- Protocol：サービスが使用するネットワーク プロトコル（tcp、udp、icmp など）。
- Source Ports：サービスが使用する送信元ポート。
- Destination Ports：サービスが使用する宛先ポート。
- ICMP Type：ICMP タイプ（たとえば、ルータ アドバタイズメントの 9 など）。
- Description（オプション）：オブジェクトの説明を指定します。
- Source/Destination/Service ボタン：フィルタ ルールまたはクエリーにアドレス オブジェクトまたはサービス オブジェクトを追加します。

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（P. 22-6）

URL フィルタリング（P. 22-1）