CHAPTER 28

フィルタリング サービスの設定

この章では、フィルタリング サービスを使用することにより、ASA を通過するトラフィックをどのように制御できるかについて説明します。次の項目を取り上げます。

Web トラフィック フィルタリングに関する情報

Web トラフィック フィルタリングは、2 つの異なる方法で使用できます。

- ActiveX オブジェクトまたは Java アプレットのフィルタリング
- 外部フィルタリング サーバを使用するフィルタリング

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 Web トラフィックから取り除くことができます。

Web トラフィック フィルタリングを使用して、Secure Computing SmartFilter（従来の N2H2）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。Web トラフィック フィルタリング用に Websense または Secure Computing SmartFilter のいずれかを使用する長い URL、HTTPS、および FTP フィルタリングをイネーブルにできます。フィルタリング 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。

（注） URL キャッシングが動作するのは、URL サーバのベンダーから提供された URL サーバ ソフトウェアのバージョンで URL キャッシングがサポートされている場合だけです。

Web トラフィック 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、外部フィルタリング サーバを使用してトラフィックをフィルタリングしている場合でも、ネットワークの速度および Web トラフィック フィルタリング サーバのキャパシティによっては、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。

モデル	ライセンス要件
すべてのモデル	基本ライセンス

外部サーバを使用した URL および FTP 要求のフィルタリング

この項では、外部サーバを使用して URL および FTP 要求をフィルタする方法について説明します。次の項目を取り上げます。

URL フィルタリングに関する情報

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。次のいずれかのインターネット フィルタリング製品で稼働する別途サーバを使用することで、設定を簡素化し、ASA 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、HTTPS、FTP、および長い URL フィルタリング用の McAfee SmartFilter（従来の N2H2）

  長い URL では、[Referer] フィールドの URL に「host:」というテキスト文字列が含まれている場合があります。これによって、HTTP GET ヘッダーが HTTP ホスト パラメータが含まれているものとして誤って解析されるおそれがあります。一方 ASA では、[Referer] フィールドに「host:」というテキスト文字列が含まれている場合でも、このフィールドを正しく解析し、正しい参照元 URL とともにヘッダーを McAfee SmartFilter サーバに転送します。

（注） URL キャッシングが動作するのは、URL サーバのベンダーから提供された URL サーバ ソフトウェアのバージョンで URL キャッシングがサポートされている場合だけです。

外部サーバを使用するときは ASA のパフォーマンスはほとんど影響を受けませんが、フィルタリング サーバが ASA から離れた場所にある場合には、Web サイトまたは FTP サーバへのアクセス時間が大幅に長くなることがあります。

フィルタリングがイネーブルで、接続要求を ASA 経由で転送すると、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 サーバによって接続が許可されると、ASA はコンテンツ サーバからの応答を発信元のクライアントに転送します。フィルタリング サーバが接続を拒否した場合、ASA 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。

ASA 上でユーザ認証がイネーブルの場合、ASA 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。

URL フィルタリングのライセンス要件

次の表に、URL フィルタリングのライセンス要件を示します。

表 28-1　ライセンスの要件

モデル	ライセンス要件
すべてのモデル	基本ライセンス

URL フィルタリングのガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

IPv6 のガイドライン

IPv6 はサポートされません。

フィルタリング サーバの指定

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。ASA 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。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。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 または HTTPS 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。

外部フィルタリング サーバを指定するには、次の手順を実行します。

ステップ 1　ASDM メイン ウィンドウで、[Configuration] > [Firewall] > [URL Filtering Servers] を選択します。

ステップ 2　[URL Filtering Server Type] 領域で、次のいずれかのオプションをクリックします。

- **Websense**
- **Secure Computing SmartFilter**

ステップ 3　2 番目のオプションを選択する際に、Secure Computing SmartFilter ポート番号がデフォルト ポート番号の 4005 ではない場合は、その番号を入力します。

ステップ 4　[URL Filtering Servers] 領域で、[Add] をクリックします。

[Websense] オプションを選択すると、[Add Parameters for Websense URL Filtering] ダイアログボックスが表示されます。

- ドロップダウン リストから、URL フィルタリング サーバが接続されているインターフェイスを選択します。
- URL フィルタリング サーバの IP アドレスを入力します。
- URL フィルタリング サーバへの要求がタイムアウトになる秒数を入力します。デフォルトは 30 秒です。
- [Protocol] 領域で、URL フィルタリング サーバとの通信に使用する TCP のバージョンを指定し、次のいずれかのオプション ボタンをクリックします。
  - TCP 1
  - TCP 4
  - UDP 4
- URL フィルタリング サーバとの通信を許可する TCP 接続の最大数を入力し、[OK] をクリックします。

新しい Websense URL フィルタリング サーバ プロパティが [URL Filtering Servers] ペインに表示されます。これらのプロパティを変更する場合は、[Edit] をクリックします。最初の Websense URL フィルタリング サーバを追加した後でさらに Websense URL フィルタリング サーバを追加する場合は、[Add] または [Insert] をクリックします。Websense URL フィルタリング サーバを削除するには、[Delete] をクリックします。

[Secure Computing SmartFilter URL Filtering] オプションを選択した場合は、[Add Parameters for Secure Computing SmartFilter URL Filtering] ダイアログボックスが表示されます。

- ドロップダウン リストから、URL フィルタリング サーバが接続されているインターフェイスを選択します。
- URL フィルタリング サーバの IP アドレスを入力します。
- URL フィルタリング サーバへの要求がタイムアウトになる秒数を入力します。デフォルトは 30 秒です。
- [Protocol] 領域で、URL フィルタリング サーバとの通信に使用するプロトコル タイプを指定し、次のいずれかのオプション ボタンをクリックします。
  - TCP
  - UDP
- URL フィルタリング サーバとの通信を許可する TCP 接続の最大数を入力し、[OK] をクリックします。

新しい Secure Computing SmartFilter URL フィルタリング サーバ プロパティが [URL Filtering Servers] ペインに表示されます。これらのプロパティを変更する場合は、[Edit] をクリックします。最初の Secure Computing SmartFilter URL フィルタリング サーバを定義した後でさらに Secure Computing SmartFilter URL フィルタリング サーバを追加する場合は、[Add] または [Insert] をクリックします。Secure Computing SmartFilter URL フィルタリング サーバを削除するには、[Delete] をクリックします。

その他の URL フィルタリング設定

ユーザが Web サイトにアクセスすると、フィルタリング サーバは ASA 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 Web 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。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場合、ASA ではサーバ アドレスを取得するためにフィルタリング 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。

この項では、その他の URL フィルタリング設定を行う方法について説明します。次の項目を取り上げます。

- 「コンテンツ サーバ応答のバッファリング」（P.28-5）
- 「サーバ アドレスのキャッシング」（P.28-6）
- 「HTTP URL のフィルタリング」（P.28-6）

コンテンツ サーバ応答のバッファリング

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、ASA 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。この動作により、Web クライアントに対する Web サーバの応答が遅れます。これは、Web 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。この動作により、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。

HTTP 要求または FTP 要求に対する応答のバッファリングを設定するには、次の手順を実行します。

ステップ 1　[URL Filtering Servers] ペインで、[Advanced] をクリックして [Advanced URL Filtering] ダイアログボックスを表示します。

ステップ 2　[URL Buffer Size] 領域で、[Enable buffering] チェックボックスをオンにします。

ステップ 3　1550 バイトのバッファ数を入力します。有効値の範囲は 1 ～ 128 です。

ステップ 4　[OK] をクリックして、このダイアログボックスを閉じます。

サーバ アドレスのキャッシング

ユーザが Web サイトにアクセスすると、フィルタリング サーバは ASA 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 Web 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。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場合、ASA ではフィルタリング 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。**url-cache** コマンドを使用する前に、Websense 実行ログを蓄積できます。

スループットを向上させるには、次の手順を実行します。

ステップ 1　[URL Filtering Servers] ペインで、[Advanced] をクリックして [Advanced URL Filtering] ダイアログボックスを表示します。

ステップ 2　[URL Cache Size] 領域で、[Enable caching based on] チェックボックスをオンにして、指定した基準に応じてキャッシングをイネーブルにします。

ステップ 3　次のいずれかのオプション ボタンをクリックします。

- [Destination Address]：このオプションを選択すると、URL 宛先アドレスに基づいてエントリがキャッシュされます。この設定は、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]：このオプションを選択すると、URL 要求を開始する送信元アドレスと URL 宛先アドレスの両方に基づいてエントリがキャッシュされます。この設定は、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。

ステップ 4　キャッシュ サイズの値を 1 ～ 128（KB）の範囲で入力します。

ステップ 5　[OK] をクリックして、このダイアログボックスを閉じます。

HTTP URL のフィルタリング

この項では、外部フィルタリング サーバを使用する HTTP フィルタリングを設定する方法について説明します。次の項目を取り上げます。

- 「長い HTTP URL のフィルタリングのイネーブル化」（P.28-6）

長い HTTP URL のフィルタリングのイネーブル化

デフォルトでは、ASA は、1159 文字を超える HTTP URL を長い URL と見なします。最大許容量を大きくすることができます。

1 つの URL の最大サイズを設定するには、次の手順を実行します。

ステップ 1　[URL Filtering Servers] ペインで、[Advanced] をクリックして [Advanced URL Filtering] ダイアログボックスを表示します。

ステップ 2　[Long URL Support] 領域で、[Use Long URL] チェックボックスをオンにして、フィルタリング サーバ用に長い URL をイネーブルにします。

ステップ 3　URL の最大許容長を 4 KB を上限として指定します。

ステップ 4　長い URL に割り当てられるメモリ量を KB 単位で入力します。

ステップ 5　[OK] をクリックして、このダイアログボックスを閉じます。

フィルタリング ルールの設定

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] の順に選択します。

フィルタリング ルールを設定するには、次の手順を実行します。

ステップ 1　ASDM メイン ウィンドウで、[Configuration] > [Firewall] > [Filter Rules] を選択します。

ステップ 2　ツールバーで [Add] をクリックし、次のリストから追加できるフィルタ ルールのタイプを表示します。

- Add Filter ActiveX Rule
- Add Filter Java Rule
- Add Filter HTTP Rule
- Add Filter HTTPS Rule
- Add Filter FTP Rule

ステップ 3　[Add Filter ActiveX Rule] を選択した場合は、次の設定を行います。

- [Filter ActiveX] または [Do not filter ActiveX] のいずれかのオプション ボタンをクリックします。
- 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入力します。宛先を入力するには、次のオプションから選択します。
  - 任意の送信元アドレスを指定するには、**any** を入力します。
  - ホスト名を入力します。
  - 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。
  - 省略符号をクリックし、[Browse Source] ダイアログボックスを表示します。ドロップダウン リストからホストまたはアドレスを選択します。
- 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入力します。宛先を入力するには、次のオプションから選択します。
  - 任意の宛先アドレスを指定するには、**any** を入力します。
  - ホスト名を入力します。
  - 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。
  - 省略符号をクリックし、[Browse Destination] ダイアログボックスを表示します。ドロップダウン リストからホストまたはアドレスを選択します。
- 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。サービスを指定するには、次のいずれかを入力します。
  - 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。

- ウェルノウン サービス名（HTTP や FTP など）を入力します。
- 省略符号をクリックし、[Browse Service] ダイアログボックスを表示します。ドロップダウン リストからサービスを選択します。

- [OK] をクリックして、このダイアログボックスを閉じます。
- [Apply] をクリックして変更内容を保存します。

ステップ 4　[Add Filter Java Rule] を選択した場合は、次の設定を行います。

- [Filter Java] または [Do not filter Java] のいずれかのオプション ボタンをクリックします。
- 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入力します。宛先を入力するには、次のオプションから選択します。
  - 任意の送信元アドレスを指定するには、**any** を入力します。
  - ホスト名を入力します。
  - 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。
  - 省略符号をクリックし、[Browse Source] ダイアログボックスを表示します。ドロップダウン リストからホストまたはアドレスを選択します。
- 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入力します。宛先を入力するには、次のオプションから選択します。
  - 任意の宛先アドレスを指定するには、**any** を入力します。
  - ホスト名を入力します。
  - 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。
  - 省略符号をクリックし、[Browse Destination] ダイアログボックスを表示します。ドロップダウン リストからホストまたはアドレスを選択します。
- 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。サービスを指定するには、次のいずれかを入力します。
  - 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。
  - ウェルノウン サービス名（HTTP や FTP など）を入力します。
  - 省略符号をクリックし、[Browse Service] ダイアログボックスを表示します。ドロップダウン リストからサービスを選択します。
- [OK] をクリックして、このダイアログボックスを閉じます。
- [Apply] をクリックして変更内容を保存します。

ステップ 5　[Add Filter HTTP Rule] を選択した場合は、次の設定を行います。

- [Filter HTTP] または [Do not filter HTTP] のいずれかのオプション ボタンをクリックします。
- 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入力します。宛先を入力するには、次のオプションから選択します。
  - 任意の送信元アドレスを指定するには、**any** を入力します。
  - ホスト名を入力します。
  - 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。
  - 省略符号をクリックし、[Browse Source] ダイアログボックスを表示します。ドロップダウン リストからホストまたはアドレスを選択します。
- 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入力します。宛先を入力するには、次のオプションから選択します。
  - 任意の宛先アドレスを指定するには、**any** を入力します。
  - ホスト名を入力します。
  - 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。
  - 省略符号をクリックし、[Browse Destination] ダイアログボックスを表示します。ドロップダウン リストからホストまたはアドレスを選択します。
- 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。サービスを指定するには、次のいずれかを入力します。
  - 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。
  - ウェルノウン サービス名（HTTP や FTP など）を入力します。
  - 省略符号をクリックし、[Browse Service] ダイアログボックスを表示します。ドロップダウン リストからサービスを選択します。
- 指定されたサイズを URL が超えた場合に実行するアクションをドロップダウン リストから選択します。
- URL フィルタリングを実行せずに接続する場合は、[Allow outbound traffic if URL server is not available] チェックボックスをオンにします。このチェックボックスをオフにすると、URL サーバが使用できない場合はインターネット Web サイトに接続できません。
- プロキシ サーバを介した HTTP 要求を禁止する場合は、[Block users from connecting to an HTTP proxy server] チェックボックスをオンにします。
- ASA がパラメータなしの 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 サーバに転送するようにする場合は、[Truncate CGI parameters from URL sent to URL server] チェックボックスをオンにします。
- [OK] をクリックして、このダイアログボックスを閉じます。
- [Apply] をクリックして変更内容を保存します。

ステップ 6　[Add Filter HTTPS Rule] を選択した場合は、次の設定を行います。

- [Filter HTTPS] または [Do not filter HTTPS] のいずれかのオプション ボタンをクリックします。

- 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入力します。宛先を入力するには、次のオプションから選択します。
  - 任意の送信元アドレスを指定するには、**any** を入力します。
  - ホスト名を入力します。
  - 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。
  - 省略符号をクリックし、[Browse Source] ダイアログボックスを表示します。ドロップダウン リストからホストまたはアドレスを選択します。
- 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入力します。宛先を入力するには、次のオプションから選択します。
  - 任意の宛先アドレスを指定するには、**any** を入力します。
  - ホスト名を入力します。
  - 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。
  - 省略符号をクリックし、[Browse Destination] ダイアログボックスを表示します。ドロップダウン リストからホストまたはアドレスを選択します。
- 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。サービスを指定するには、次のいずれかを入力します。
  - 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。
  - ウェルノウン サービス名（HTTP や FTP など）を入力します。
  - 省略符号をクリックし、[Browse Service] ダイアログボックスを表示します。ドロップダウン リストからサービスを選択します。
- URL フィルタリングを実行せずに接続する場合は、[Allow outbound traffic if URL server is not available] チェックボックスをオンにします。このチェックボックスをオフにすると、URL サーバが使用できない場合はインターネット Web サイトに接続できません。
- [OK] をクリックして、このダイアログボックスを閉じます。
- [Apply] をクリックして変更内容を保存します。

ステップ 7　[Add Filter FTP Rule] を選択した場合は、次の設定を行います。

- [Filter FTP] または [Do not filter FTP] のいずれかのオプション ボタンをクリックします。
- 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入力します。宛先を入力するには、次のオプションから選択します。
  - 任意の送信元アドレスを指定するには、**any** を入力します。
  - ホスト名を入力します。
  - 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。

  - 省略符号をクリックし、[Browse Source] ダイアログボックスを表示します。ドロップダウン リストからホストまたはアドレスを選択します。
- 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入力します。宛先を入力するには、次のオプションから選択します。
  - 任意の宛先アドレスを指定するには、**any** を入力します。
  - ホスト名を入力します。
  - 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。
  - 省略符号をクリックし、[Browse Destination] ダイアログボックスを表示します。ドロップダウン リストからホストまたはアドレスを選択します。
- 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。サービスを指定するには、次のいずれかを入力します。
  - 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。
  - ウェルノウン サービス名（http や ftp など）を入力します。
  - 省略符号をクリックし、[Browse Service] ダイアログボックスを表示します。ドロップダウン リストからサービスを選択します。
- URL フィルタリングを実行せずに接続する場合は、[Allow outbound traffic if URL server is not available] チェックボックスをオンにします。このチェックボックスをオフにすると、URL サーバが使用できない場合はインターネット Web サイトに接続できません。
- FTP ディレクトリへの相対パス名を使用している FTP 要求をドロップする場合は、[Block interactive FTP sessions (block if absolute FTP path is not provided)] チェックボックスをオンにします。
- [OK] をクリックして、このダイアログボックスを閉じます。
- [Apply] をクリックして変更内容を保存します。

ステップ 8　フィルタリング ルールを変更するには、ルールを選択し、[Edit] をクリックして、指定したフィルタリング ルールの [Edit Filter Rule] ダイアログボックスを表示します。

ステップ 9　必要な変更を加え、[OK] をクリックしてこのダイアログボックスを閉じます。

ステップ 10　[Apply] をクリックして変更内容を保存します。

ルール テーブルのフィルタリング

ルール テーブルに多数のエントリが含まれている場合に特定のルールを見つけるには、ルール テーブルにフィルタを適用して、フィルタで指定したルールのみを表示できます。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、[Filter] ツールバーを表示します。

ステップ 2　[Filter] ドロップダウン リストから、次のフィルタ 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.　照合する文字列を次のいずれかの方法で入力します。

- 隣のフィールドに、送信元、宛先、またはサービスの名前を入力します。
- 省略符号をクリックすると [Browse] ダイアログボックスが開き、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。

b.　ドロップダウン 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] を、部分一致させるには [contains] を選択します。

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] をクリックします。クエリーを定義するには、「クエリーの定義」（P.28-12）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削除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。

ステップ 8　選択したルールのパケット トレースを表示するには、[Packet Trace] をクリックします。

ステップ 9　選択したルール図を表示および非表示にするには、[Diagram] をクリックします。

ステップ 10　フィルタ ルールを削除して別の場所に配置するには、[Cut] をクリックします。

ステップ 11　フィルタ ルールをコピーするには、[Copy] をクリックします。次にコピーしたフィルタ ルールを別の場所に貼り付けるには、[Paste] をクリックします。

ステップ 12　選択したフィルタ ルールを削除するには、[Delete] をクリックします。

クエリーの定義

クエリーを定義するには、次の手順を実行します。

ステップ 1　送信元の IP アドレスまたはホスト名を入力します。完全一致には [is]、部分一致には [contains] を選択します。省略符号をクリックし、[Browse Source] ダイアログボックスを表示します。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。

ステップ 2　宛先の IP アドレスまたはホスト名を入力します。完全一致には [is]、部分一致には [contains] を選択します。省略符号をクリックし、[Browse Destination] ダイアログボックスを表示します。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。

ステップ 3　送信元または宛先の IP アドレスまたはホスト名を入力します。完全一致には [is]、部分一致には [contains] を選択します。省略符号をクリックし、[Browse Source] ダイアログボックスを表示します。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。

ステップ 4　サービスのプロトコル、ポート、または名前を入力します。完全一致には [is]、部分一致には [contains] を選択します。省略符号をクリックし、[Browse Service] ダイアログボックスを表示します。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。

ステップ 5　ドロップダウン リストから、ルール タイプを選択します。

ステップ 6　[OK] をクリックして、このダイアログボックスを閉じます。

[OK] をクリックすると、フィルタがただちにルール テーブルに適用されます。フィルタを削除するには、[Clear] をクリックします。

URL フィルタリングの機能履歴

表 28-2 に、URL フィルタリングのリリース履歴の一覧を示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 28-2　URL フィルタリングの機能履歴

機能名	プラットフォーム リリース	機能情報
URL フィルタリング	7.0(1)	設定された一連のフィルタリング基準に基づいて URL をフィルタします。