CHAPTER 23

サービス ポリシー ルールの設定

この章では、サービス ポリシー ルールをイネーブルにする方法を説明します。サービス ポリシーを使用すると、一貫した柔軟な方法でセキュリティ アプライアンスの機能を設定できます。たとえば、サービス ポリシーを使用して、すべての TCP アプリケーションに適用されるタイムアウト コンフィギュレーションを作成する一方で、特定の TCP アプリケーションに固有のタイムアウト コンフィギュレーションを作成できます。

この章には、次の項があります。

サービス ポリシーの概要

この項では、セキュリティ ポリシーの概要について説明します。次の項目を取り上げます。

サポートされている機能

セキュリティ ポリシーは次の機能をサポートします。

- TCP 正規化、TCP および UDP の接続制限とタイムアウト、および TCP シーケンス番号のランダム化
- CSC
- アプリケーション検査
- IPS
- QoS 入力ポリシング
- QoS 出力ポリシング
- QoS プライオリティキュー

サービス ポリシーの要素

サービス ポリシーの設定では、インターフェイスあたりのサービス ポリシー ルール、またはグローバル ポリシーのサービス ポリシー ルールを 1 つ以上追加します。それぞれのルールごとに、次の要素を指定します。

1. ルールを適用するインターフェイスを指定するか、またはグローバル ポリシーを指定します。
2. アクションを適用するトラフィックを指定します。レイヤ 3 および 4 の通過トラフィックを指定できます。
3. トラフィック クラスにアクションを適用します。トラフィック クラスごとに複数のアクションを適用できます。

デフォルトのグローバル ポリシー

コンフィギュレーションには、すべてのデフォルト アプリケーション検査トラフィックを照合し、特定の検査をすべてのインターフェイスのトラフィックに適用するポリシー（グローバル ポリシー）がデフォルトで含まれています。すべての検査がデフォルトでイネーブルになっているわけではありません。1 つのグローバル ポリシーしか適用できないため、グローバル ポリシーを変更する場合には、デフォルト ポリシーを編集するか、またはそのポリシーをディセーブルにして新しいポリシーを適用する必要があります（インターフェイス ポリシーはグローバル ポリシーより優先されます）。

デフォルト ポリシーには次のアプリケーション検査が含まれています。

- 最大メッセージ長 512 バイトに対する DNS 検査
- FTP
- H323（H225）

- H323（RAS）
- RSH
- RTSP
- ESMTP
- SQLnet
- Skinny（SCCP）
- SunRPC
- XDMCP
- SIP
- NetBIOS
- TFTP

機能の方向性

アクションは、機能に応じて双方向または単方向でトラフィックに適用されます。双方向で適用される機能の場合には、トラフィックが両方の方向でクラスマップを照合するのであれば、ポリシーマップを適用するインターフェイスに出入りするすべてのトラフィックが影響を受けます。

（注）　グローバル ポリシーを使用する場合は、すべての機能が単方向になります。1 つのインターフェイスに適用されるときには通常であれば双方向の機能も、グローバルに適用されるときは各インターフェイスの入力側にのみ適用されます。グローバルポリシーはすべてのインターフェイスに適用されるため、両方向で適用されることになります。このため、この場合の双方向性は冗長になります。

たとえば QoS プライオリティキューのように単方向で適用される機能の場合は、ポリシー マップを適用するインターフェイスから出る側のトラフィックのみが影響を受けます。各機能の方向性については、表 23-1 を参照してください。

表 23-1　機能の方向性

機能	単一インターフェイス方向	グローバル方向
TCP 正規化、TCP および UDP の接続制限とタイムアウト、および TCP シーケンス番号のランダム化	双方向	入力側
CSC	双方向	入力側
アプリケーション検査	双方向	入力側
IPS	双方向	入力側
QoS 入力ポリシング	入力側	入力側
QoS 出力ポリシング	出力側	出力側
QoS プライオリティキュー	出力側	出力側

複数サービス ポリシーの場合の機能照合ガイドライン

TCP および UDP トラフィック（および、ステートフル ICMP 検査がイネーブルの場合の ICMP）の場合、サービス ポリシーは、個々のパケットだけでなくトラフィック フローにも適用されます。トラフィックが 1 つのインターフェイスのポリシーで定義されている機能を照合する既存接続の一部になっている場合、そのトラフィック フローは、別のインターフェイスのポリシーで定義されている同じ機能を照合できません。最初のポリシーのみが使用されます。

たとえば、HTTP トラフィックが HTTP トラフィックを検査する内部インターフェイスのポリシーを照合し、HTTP 検査を行う外部インターフェイスで別個のポリシーが定義されている場合、そのトラフィックが外部インターフェイスの出力側でも検査されることはありません。同様に、その接続のリターン トラフィックは、外部インターフェイスの入力側ポリシーによって検査されたり、内部インターフェイスの出力側ポリシーによって検査されたりすることもありません。

ステートフル ICMP 検査をイネーブルにしない場合の ICMP のようにフローとして処理されないトラフィックの場合、リターン トラフィックは戻りインターフェイスの別のポリシー マップを照合できます。たとえば、内部および外部インターフェイスで IPS 検査を設定するときに、内部ポリシーでは仮想センサー 1 を使用するのに対して、外部ポリシーでは仮想センサー 2 を使用する場合、非ステートフル ping は仮想センサー 1 の発信側を照合するだけでなく、仮想センサー 2 の着信側も照合します。

ルール内の複数の機能アクションが適用される順序

ルール内のアクションは、次の順序で実行されます。

- TCP 正規化、TCP および UDP の接続制限とタイムアウト、および TCP シーケンス番号のランダム化

（注） セキュリティ アプライアンスがプロキシ サービス（AAA や CSC など）を実行する場合、または TCP ペイロード（FTP 検査など）を変更する場合、TCP ノーマライザはデュアル モードで動作します。このモードでは、プロキシまたはペイロード変更サービスの前後にアクションが適用されます。

- CSC
- アプリケーション検査
- IPS
- QoS 入力ポリシング
- QoS 出力ポリシング
- QoS プライオリティキュー

通過トラフィックのサービス ポリシー ルールの追加

通過トラフィックのサービス ポリシー ルールを追加するには、次の手順を実行します。

ステップ 1　Configuration > Firewall > Service Policy Rules ペインで、**Add** をクリックします。

Add Service Policy Rule Wizard - Service Policy ダイアログボックスが表示されます。

（注）　Add　ボタンの右側にある小さな矢印ではなく　Add　ボタンをクリックすると、通過トラフィック ルールがデフォルトで追加されます。Add ボタン上の矢印をクリックすると、通過トラフィック ルールと管理トラフィック ルールのいずれかを選択できます。

ステップ 2　Create a Service Policy and Apply To 領域で、次のオプションの 1 つをクリックします。

- **Interface**。このオプションでは、サービス ポリシーが 1 つのインターフェイスに適用されます。インターフェイス ポリシーはグローバル ポリシーより優先されます。
  - **a.** ドロップダウン リストからインターフェイスを選択します。

    すでにポリシーが適用されているインターフェイスを選択する場合は、ウィザードの指示に従って、新しいサービス ポリシー ルールをそのインターフェイスに追加できます。
  - **b.** 新しいサービス ポリシーの場合は、Policy Name フィールドに名前を入力します。
  - **c.**（オプション）Description フィールドに説明を入力します。
- **Global - applies to all interfaces**。このオプションでは、サービス ポリシーがすべてのインターフェイスにグローバルに適用されます。デフォルト アプリケーション検査のサービス ポリシー ルールを含むグローバル ポリシーは、デフォルトで存在します。詳細については、P.23-2 の「デフォルトのグローバル ポリシー」を参照してください。ウィザードを使用してルールをグローバル ポリシーに追加できます。

ステップ 3　**Next** をクリックします。

Add Service Policy Rule Wizard - Traffic Classification Criteria ダイアログボックスが表示されます。

ステップ 4　次のオプションのいずれかをクリックして、ポリシーのアクションを適用するトラフィックを指定します。

- **Create a new traffic class**。Create a new traffic class フィールドにトラフィック クラス名を入力し、説明（オプション）を入力します。

  基準のいずれかを使用してトラフィックを特定します。
  - **Default Inspection Traffic**：クラスは、セキュリティ アプライアンスが検査可能なすべてのアプリケーションによって使用される、デフォルトの TCP および UDP ポートを照合します。

    デフォルト ポートの一覧については、P.24-3 の「デフォルトの検査ポリシー」を参照してください。セキュリティ アプライアンスには、デフォルト検査トラフィックを照合し、すべてのインターフェイスのトラフィックに共通検査を適用するグローバル ポリシーが組み込まれています。Default Inspection Traffic クラスにポートが含まれているすべてのアプリケーションが、ポリシー マップにおいてデフォルトでイネーブルになっているわけではありません。

Source and Destination IP Address (uses ACL) クラスを Default Inspection Traffic クラスと一緒に指定して、照合されるトラフィックを絞り込むことができます。Default Inspection Traffic クラスによって照合するポートが指定されるため、アクセスリストのポートはすべて無視されます。

- **Source and Destination IP Address (uses ACL)**：このクラスは拡張アクセスリストで指定されているトラフィックを照合します。セキュリティ アプライアンスが透過ファイアウォール モードで動作している場合は、EtherType アクセスリストを使用できます。

（注） このタイプの新しいトラフィック クラスを作成する場合は、最初にアクセス コントロール エントリ（ACE）を 1 つのみ指定できます。ルールを追加した後は、同じインターフェイスまたはグローバル ポリシーに新しいルールを追加し、それから Traffic Classification ダイアログボックス（以下を参照）で **Add rule to existing traffic class** を指定することによって、ACE を追加できます。

- **Tunnel Group**：このクラスは、QoS を適用するトンネル グループのトラフィックを照合します。その他にもう 1 つのトラフィック照合オプションを指定してトラフィック照合対象をさらに絞込み、Any Traffic、Source and Destination IP Address (uses ACL)、または Default Inspection Traffic を排除できます。
- **TCP or UDP Destination Port**：このクラスは、1 つのポートまたは連続する一定範囲のポートを照合します。

ヒント 複数の非連続ポートを使用するアプリケーションの場合は、Source and Destination IP Address (uses ACL) を使用して各ポートを照合します。

- **RTP Range**：このクラス マップは RTP トラフィックを照合します。
- **IP DiffServ CodePoints (DSCP)**：このクラスは、IP ヘッダーの最大 8 つの DSCP 値を照合します。
- **IP Precedence**：このクラス マップは、IP ヘッダーの TOS バイトによって表される、最大 4 つの Precedence 値を照合します。
- **Any Traffic**：すべてのトラフィックを照合します。

- **Add rule to existing traffic class**。すでに同じインターフェイスにサービス ポリシー ルールを指定している場合、またはグローバル サービス ポリシーを追加する場合は、このオプションによって既存のアクセスリストに ACE を追加できます。このインターフェイスのサービス ポリシー ルールで Source and Destination IP Address (uses ACL) オプションを選択した場合は、事前に作成したすべてのアクセスリストに ACE を追加できます。このトラフィック クラスでは、複数の ACE を追加する場合であっても、1 セットのルール アクションしか指定できません。この手順全体を繰り返すことによって、複数の ACE を同じトラフィック クラスに追加できます。ACE の順序の変更方法については、P.23-13 の「サービス ポリシー ルールの順序の管理」を参照してください。
- **Use an existing traffic class**。別のインターフェイスのルールで使用されるトラフィック クラスを作成した場合は、そのトラフィック クラス定義をこのルールで再使用できます。1 つのルールのトラフィック クラスを変更すると、その変更は同じトラフィック クラスを使用するすべてのルールに継承されます。コンフィギュレーションに CLI で入力した **class-map** コマンドが含まれている場合は、それらのトラフィック クラス名も使用できます（ただし、そのトラフィック クラスの定義を表示するには、そのルールを作成する必要があります）。

- **Use class default as the traffic class**。このオプションでは、すべてのトラフィックを照合する class-default クラスを使用します。class-default クラスは、セキュリティ アプライアンスによって自動的に作成され、ポリシーの最後に配置されます。このクラスは、アクションを何も適用しない場合でもセキュリティ アプライアンスによって作成されますが、内部での使用に限られます。必要に応じて、このクラスにアクションを適用できます。これは、すべてのトラフィックを照合する新しいトラフィック クラスを作成するよりも便利な場合があります。class-default クラスを使用して、このサービス ポリシーにルールを 1 つだけ作成できます。これは、各トラフィック クラスを関連付けることができるのは、サービス ポリシーごとに 1 つのルールだけであるためです。

ステップ 5　**Next** をクリックします。

ステップ 6　次に表示されるダイアログボックスは、選択したトラフィック照合基準に応じて異なります。

（注） Any Traffic オプションの場合には、追加設定を行うための特別なダイアログボックスはありません。

- Default Inspections：このダイアログボックスは情報提供の目的でのみ表示され、トラフィック クラスに含まれるアプリケーションとポートが示されます。
- Source and Destination Address：このダイアログボックスでは、送信元アドレスと宛先アドレスを設定できます。

  a. **Match** または **Do Not Match** をクリックします。

  Match オプションでは、アドレスが一致するトラフィックにアクションを適用する場合のルールを作成します。Do Not Match オプションでは、トラフィックを指定したアクションの適用から免除します。たとえば、10.1.1.25 を除いて、10.1.1.0/24 のトラフィックすべてを照合し、そのトラフィックに接続制限を適用するとします。この場合は、2 つのルール（Match オプションを使用した 10.1.1.0/24 に対するルールおよび Do Not Match オプションを使用した 10.1.1.25 に対するルール）を作成します。必ず、Do Not Match ルールが Match ルールの上になるように配置してください。順序を逆にすると、10.1.1.25 が最初に Match ルールを照合することになります。

  b. Source フィールドで、送信元 IP アドレスを入力するか、**...** ボタンをクリックして ASDM にすでに定義されている IP アドレスを選択します。

  プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

  任意の送信元アドレスを指定するには、**any** を入力します。

  アドレスが複数ある場合はカンマで区切ります。

  c. Destination フィールドで、宛先 IP アドレスを入力するか、**...** ボタンをクリックして ASDM にすでに定義されている IP アドレスを選択します。

  プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

  任意の宛先アドレスを指定するには、**any** を入力します。

  アドレスが複数ある場合はカンマで区切ります。

  d. Service フィールドで、宛先サービスの IP サービス名または番号を入力するか、**...** ボタンをクリックしてサービスを選択します。

  TCP または UDP のポート番号、あるいは ICMP サービス番号を指定する場合は、*プロトコル/ポート*を入力します。たとえば、TCP/8080 と入力します。

  デフォルトでは、サービスは IP です。

  サービスが複数ある場合はカンマで区切ります。

e. （オプション）Description フィールドに説明を入力します。

f. （オプション）TCP または UDP の送信元サービスを指定するには、**More Options** 領域をクリックして開き、Source Service フィールドに TCP サービスまたは UDP サービスを入力します。

宛先サービスと送信元サービスは同じである必要があります。Destination Service フィールドをコピーし、Source Service フィールドに貼り付けます。

g. （オプション）ルールを非アクティブにするには、**More Options** 領域をクリックして開き、**Enable Rule** をオフにします。

この設定は、ルールを削除せずに無効にしたい場合に便利です。

h. （オプション）ルールの時間範囲を指定するには、**More Options** 領域をクリックして開き、Time Range ドロップダウン リストから時間範囲を選択します。

新しい時間範囲を追加するには、**...** ボタンをクリックします。詳細については、P.8-16 の「時間範囲の設定」を参照してください。

この設定は、事前に設定した時間にだけルールをアクティブにする場合に便利です。

- Tunnel Group：Tunnel Group ドロップダウン リストからトンネル グループを選択するか、または **New** をクリックして新しいトンネル グループを追加します。詳細については、P.32-65 の「Add IPSec Remote Access Connection and Add SSL VPN Access Connection」を参照してください。

各フローをポリシングするには、**Match flow destination IP address** をオンにします。一意の IP 宛先アドレスに向かうすべてのトラフィックは、フローとみなされます。

- Destination Port：**TCP** または **UDP** をクリックします。

Service フィールドに、ポート番号または名前を入力するか、または **...** をクリックして ASDM で定義済みのサービスを選択します。

- RTP Range：2000 ～ 65534 の範囲で RTP ポート範囲を入力します。範囲内のポートの最大番号は 16383 です。
- IP DiffServ CodePoints (DSCP)：DSCP Value to Add 領域で、**Select Named DSCP Values** から値を選択するか、または **Enter DSCP Value (0-63)** フィールドに値を入力し、**Add** をクリックします。

必要に応じて値を追加するか、または **Remove** ボタンを使用して値を削除します。

- IP Precedence：Available IP Precedence 領域で値を選択し、**Add** をクリックします。

必要に応じて値を追加するか、または **Remove** ボタンを使用して値を削除します。

ステップ 7　**Next** をクリックします。

Add Service Policy Rule - Rule Actions ダイアログボックスが表示されます。

ステップ 8　次の章または項の説明に従って、1 つ以上のルール アクションを設定します。

- 第 24 章「アプリケーション レイヤ プロトコル検査の設定」
- P.27-7 の「接続の設定」
- P.28-3 の「QoS タブのフィールド情報」
- 第 39 章「IPS の設定」
- 第 40 章「Trend Micro Content Security の設定」

ステップ 9　**Finish** をクリックします。

管理トラフィックのサービス ポリシー ルールの追加

管理目的でセキュリティ アプライアンスに転送されるトラフィックのサービス ポリシーを作成できます。このタイプのセキュリティ ポリシーでは、RADIUS アカウンティング検査と接続制限を実行できます。ここでは、次の項目について説明します。

RADIUS Accounting 検査の概要

よく知られた問題の中に、GPRS ネットワークでの過剰請求攻撃があります。過剰請求攻撃により消費者は、利用したことのないサービスについて請求されるために怒り、困惑します。この場合、悪意の攻撃者はサーバへの接続をセットアップし、SGSN から IP アドレスを取得します。攻撃者がコールを終了しても、悪意のあるサーバはそのアドレスにパケットを送信し続け、そのパケットは GGSN によってドロップされますが、悪意のあるサーバからの接続はアクティブなままの状態になります。悪意の攻撃者に割り当てられた IP アドレスは、解放されて正規のユーザに再度割り当てられ、そのユーザは攻撃者が利用したサービスについて請求されることになります。

RADIUS アカウンティング検査では、GGSN によって検出されるトラフィックが正規のものであることを確認することによって、このタイプの攻撃を防止します。RADIUS アカウンティング機能を適正に設定していると、セキュリティ アプライアンスは、Radius Accounting Request Start メッセージの Framed IP アトリビュートと Radius Accounting Request Stop メッセージの Framed IP アトリビュートの照合結果に基づいて接続を切断します。Stop メッセージで Framed IP アトリビュートの照合 IP アドレスが確認されると、セキュリティ アプライアンスは、その IP アドレスと一致する送信元との接続すべてを検索します。

RADIUS サーバで事前共有キーを設定してセキュリティ アプライアンスがメッセージを検証できるようにするオプションも用意されています。共有秘密が設定されていない場合、セキュリティ アプライアンスではメッセージの送信元を検証する必要がなく、送信元 IP アドレスが RADIUS メッセージの送信を許可されている設定済みアドレスの 1 つかどうかだけがチェックされます。

管理トラフィックのサービス ポリシー ルールの設定

管理トラフィックのサービス ポリシーを追加するには、次の手順を実行します。

ステップ 1　Configuration > Firewall > Service Policy Rules ペインで、Add の横の下矢印をクリックします。

ステップ 2　**Add Management Service Policy Rule** を選択します。

Add Management Service Policy Rule Wizard - Service Policy ダイアログボックスが表示されます。

ステップ 3　Create a Service Policy and Apply To 領域で、次のオプションの 1 つをクリックします。

- **Interface**。このオプションでは、サービス ポリシーが 1 つのインターフェイスに適用されます。インターフェイス ポリシーはグローバル ポリシーより優先されます。
  - **a.** ドロップダウン リストからインターフェイスを選択します。

    すでにポリシーが適用されているインターフェイスを選択する場合は、ウィザードの指示に従って、新しいサービス ポリシー ルールをそのインターフェイスに追加できます。
  - **b.** 新しいサービス ポリシーの場合は、Policy Name フィールドに名前を入力します。
  - **c.**（オプション）Description フィールドに説明を入力します。

- **Global - applies to all interfaces**。このオプションでは、サービス ポリシーがすべてのインターフェイスにグローバルに適用されます。デフォルト アプリケーション検査のサービス ポリシー ルールを含むグローバル ポリシーは、デフォルトで存在します。詳細については、P.23-2 の「デフォルトのグローバル ポリシー」を参照してください。ウィザードを使用してルールをグローバル ポリシーに追加できます。

ステップ 4　**Next** をクリックします。

Add Management Service Policy Rule Wizard - Traffic Classification Criteria ダイアログボックスが表示されます。

ステップ 5　次のオプションのいずれかをクリックして、ポリシーのアクションを適用するトラフィックを指定します。

- **Create a new traffic class**。Create a new traffic class フィールドにトラフィック クラス名を入力し、説明（オプション）を入力します。

  基準のいずれかを使用してトラフィックを特定します。

  - **Source and Destination IP Address (uses ACL)**：このクラスは拡張アクセスリストで指定されているトラフィックを照合します。セキュリティ アプライアンスが透過ファイアウォール モードで動作している場合は、EtherType アクセスリストを使用できます。

（注）　このタイプの新しいトラフィック クラスを作成する場合は、最初にアクセス コントロール エントリ（ACE）を 1 つのみ指定できます。ルールを追加した後は、同じインターフェイスまたはグローバル ポリシーに新しいルールを追加し、それから Traffic Classification ダイアログボックス（以下を参照）で **Add rule to existing traffic class** を指定することによって、ACE を追加できます。

  - **TCP or UDP Destination Port**：このクラスは、1 つのポートまたは連続する一定範囲のポートを照合します。

ヒント　複数の非連続ポートを使用するアプリケーションの場合は、Source and Destination IP Address (uses ACL) を使用して各ポートを照合します。

- **Add rule to existing traffic class**。すでに同じインターフェイスにサービス ポリシー ルールを指定している場合、またはグローバル サービス ポリシーを追加する場合は、このオプションによって既存のアクセスリストに ACE を追加できます。このインターフェイスのサービス ポリシー ルールで Source and Destination IP Address (uses ACL) オプションを選択した場合は、事前に作成したすべてのアクセスリストに ACE を追加できます。このトラフィック クラスでは、複数の ACE を追加する場合であっても、1 セットのルール アクションしか指定できません。この手順全体を繰り返すことによって、複数の ACE を同じトラフィック クラスに追加できます。ACE の順序の変更方法については、P.23-13 の「サービス ポリシー ルールの順序の管理」を参照してください。
- **Use an existing traffic class**。別のインターフェイスのルールで使用されるトラフィック クラスを作成した場合は、そのトラフィック クラス定義をこのルールで再使用できます。1 つのルールのトラフィック クラスを変更すると、その変更は同じトラフィック クラスを使用するすべてのルールに継承されます。コンフィギュレーションに CLI で入力した **class-map** コマンドが含まれている場合は、それらのトラフィック クラス名も使用できます（ただし、そのトラフィック クラスの定義を表示するには、そのルールを作成する必要があります）。

ステップ 6　**Next** をクリックします。

ステップ 7　次に表示されるダイアログボックスは、選択したトラフィック照合基準に応じて異なります。

- Source and Destination Address：このダイアログボックスでは、送信元アドレスと宛先アドレスを設定できます。

  a. **Match** または **Do Not Match** をクリックします。

     Match オプションでは、アドレスが一致するトラフィックにアクションを適用する場合のルールを作成します。Do Not Match オプションでは、トラフィックを指定したアクションの適用から免除します。たとえば、10.1.1.25 を除いて、10.1.1.0/24 のトラフィックすべてを照合し、そのトラフィックに接続制限を適用するとします。この場合は、2 つのルール（Match オプションを使用した 10.1.1.0/24 に対するルールおよび Do Not Match オプションを使用した 10.1.1.25 に対するルール）を作成します。必ず、Do Not Match ルールが Match ルールの上になるように配置してください。順序を逆にすると、10.1.1.25 が最初に Match ルールを照合することになります。

  b. Source フィールドで、送信元 IP アドレスを入力するか、**...** ボタンをクリックして ASDM にすでに定義されている IP アドレスを選択します。

     プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

     任意の送信元アドレスを指定するには、**any** を入力します。

     アドレスが複数ある場合はカンマで区切ります。

  c. Destination フィールドで、宛先 IP アドレスを入力するか、**...** ボタンをクリックして ASDM にすでに定義されている IP アドレスを選択します。

     プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

     任意の宛先アドレスを指定するには、**any** を入力します。

     アドレスが複数ある場合はカンマで区切ります。

  d. Service フィールドで、宛先サービスの IP サービス名または番号を入力するか、**...** ボタンをクリックしてサービスを選択します。

     TCP または UDP のポート番号、あるいは ICMP サービス番号を指定する場合は、*プロトコル/ポート*を入力します。たとえば、TCP/8080 と入力します。

     デフォルトでは、サービスは IP です。

     サービスが複数ある場合はカンマで区切ります。

  e. （オプション）Description フィールドに説明を入力します。

  f. （オプション）TCP または UDP の送信元サービスを指定するには、**More Options** 領域をクリックして開き、Source Service フィールドに TCP サービスまたは UDP サービスを入力します。

     宛先サービスと送信元サービスは同じである必要があります。Destination Service フィールドをコピーし、Source Service フィールドに貼り付けます。

  g. （オプション）ルールを非アクティブにするには、**More Options** 領域をクリックして開き、**Enable Rule** をオフにします。

     この設定は、ルールを削除せずに無効にしたい場合に便利です。

  h. （オプション）ルールの時間範囲を指定するには、**More Options** 領域をクリックして開き、Time Range ドロップダウン リストから時間範囲を選択します。

     新しい時間範囲を追加するには、**...** ボタンをクリックします。詳細については、P.8-16 の「時間範囲の設定」を参照してください。

     この設定は、事前に設定した時間にだけルールをアクティブにする場合に便利です。

- Destination Port：**TCP** または **UDP** をクリックします。

  Service フィールドに、ポート番号または名前を入力するか、または **...** をクリックして ASDM で定義済みのサービスを選択します。

ステップ 8　**Next** をクリックします。

Add Management Service Policy Rule - Rule Actions ダイアログボックスが表示されます。

ステップ 9　RADIUS アカウンティング検査を設定するには、RADIUS Accounting Map ドロップダウン リストから検査マップを選択するか、または **Configure** をクリックしてマップを追加します。

詳細については、P.23-14 の「RADIUS アカウンティング フィールドの説明」を参照してください。

ステップ 10　最大接続数を設定するには、Maximum Connections 領域で次の値を 1 つ以上入力します。

- **TCP & UDP Connections**：トラフィック クラスのすべてのクライアントで同時に接続される TCP および UDP 接続の最大数を 65,536 までの範囲で指定します。どちらのプロトコルともデフォルトは **0** で、接続可能な最大許容数に設定されています。
- **Embryonic Connections**：初期接続の最大数を 65,536 までの範囲で指定します。初期接続は、送信元と宛先の間で必要なハンドシェイクを終了していない接続要求です。この制限により、TCP 代行受信機能をイネーブルにします。デフォルトは **0** で、最大初期接続数であることを示します。TCP 代行受信により、TCP SYN パケットによってインターフェイスをフラッディングさせる DoS 攻撃から内部システムを保護します。初期接続の制限値を超えると、クライアントからセキュリティ レベルのより高いサーバへ送信される TCP SYN パケットが TCP 代行受信機能によって代行受信されます。SYN クッキーは、検証プロセス中に使用され、ドロップされる有効なトラフィックの量を最小限に抑えるのに役立ちます。したがって、到達不能なホストからの接続試行がサーバに到達することはありません。

ステップ 11　**Finish** をクリックします。

サービス ポリシー ルールの順序の管理

インターフェイス上またはグローバル ポリシー内でのサービス ポリシー ルールの順序は、トラフィックへのアクションの適用方法に影響します。パケットがサービス ポリシーのルールを照合する方法については、次のガイドラインを参照してください。

- パケットは、機能タイプごとにサービス ポリシーのルールを 1 つのみ照合できます。
- パケットが、1 つの機能タイプのアクションを含むルールを照合する場合、セキュリティ アプライアンスは、その機能タイプを含む、後続のどのルールに対してもそのパケットを照合しません。
- ただし、そのパケットが異なる機能タイプの後続のルールを照合する場合、セキュリティ アプライアンスは後続ルールのアクションも適用します。

たとえば、パケットが接続制限のルールを照合し、アプリケーション検査のルールも照合する場合は、両方のアクションが適用されます。

パケットがアプリケーション検査のルールを照合し、アプリケーション検査を含む別のルールを照合する場合、2 番目のルール アクションは適用されません。

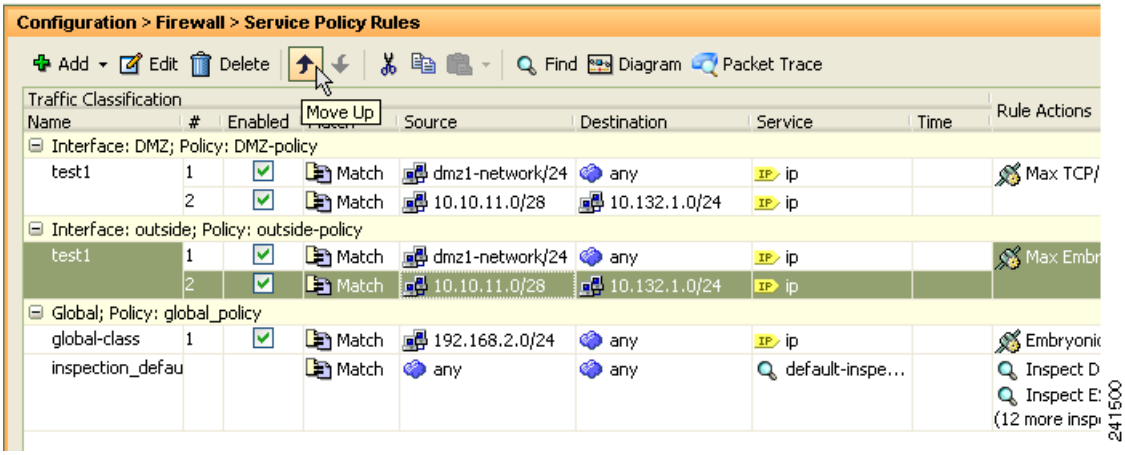
ルールに複数の ACE が組み込まれたアクセスリストが含まれる場合は、ACE の順序もパケット フローに影響します。FWSM は、リストのエントリの順序に従って、各 ACE に対してパケットをテストします。一致が検出されると、それ以後の ACE はチェックされません。たとえば、すべてのトラフィックを明示的に許可するアクセスリストの先頭に ACE を作成すると、それ以外の文はチェックされません。

ルールまたはルール内での ACE の順序を変更するには、次の手順を実行します。

ステップ 1　Configuration > Firewall > Service Policy Rules ペインで、上または下に動かすルールまたは ACE を選択します。

ステップ 2　Move Up または Move Down カーソルをクリックします（図 23-1 を参照してください）。

図 23-1　ACE の移動



（注）　複数のサービス ポリシーで使用されるアクセスリストで ACE を並べ替えると、その変更はすべてのサービス ポリシーで継承されます。

ステップ 3　ルールまたは ACE を並べ替えたら、**Apply** をクリックします。

RADIUS アカウンティング フィールドの説明

この項では、RADIUS アカウンティング フィールドの一覧を示します。次の項目を取り上げます。

Select RADIUS Accounting Map

Select RADIUS Accounting Map ダイアログボックスでは、定義済み RADIUS アカウンティング マップを選択するか、新しい RADIUS アカウンティング マップを定義できます。

フィールド

- **Add**：新しい RADIUS アカウンティング マップを追加できます。

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 RADIUS Accounting Policy Map

Add RADIUS Accounting Policy Map ダイアログボックスでは、RADIUS アカウンティング マップの基本設定を追加できます。

フィールド

- Name：事前設定されている RADIUS アカウンティング マップの名前を入力します。
- Description：RADIUS アカウンティング マップの説明を 100 文字以内で入力します。
- Host Parameters タブ：
  - Host IP Address：RADIUS メッセージの送信元となるホストの IP アドレスを指定します。
  - Key: (optional)：キーを指定します。
  - Add：Host テーブルにホスト エントリを追加します。
  - Delete：Host テーブルからホスト エントリを削除します。
- Other Parameters タブ：
  - Attribute Number：Accounting Start を受信したときに確認するアトリビュート番号を指定します。

- Add：Attribute テーブルにエントリを追加します。
- Delete：Attribute テーブルからエントリを削除します。
- Send response to the originator of the RADIUS message：RADIUS メッセージの送信元ホストにメッセージを返信します。
- Enforce timeout：ユーザのタイムアウトをイネーブルにします。

• Users Timeout：データベース内のユーザのタイムアウト（hh:mm:ss）。

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
•	•	•	•	—

RADIUS Inspect Map

RADIUS ペインでは、事前に設定された RADIUS アプリケーション検査マップを表示できます。RADIUS マップでは、RADIUS アプリケーション検査で使用されるコンフィギュレーションのデフォルト値を変更できます。RADIUS マップを使用すると、過剰請求攻撃を防御できます。

フィールド

- Name：検査マップの名前を 40 文字以内で入力します。
- Description：検査マップの説明を 200 文字以内で入力します。
- RADIUS Inspect Maps：定義されている RADIUS 検査マップを一覧表示するテーブルです。定義されている検査マップは、Inspect Maps ツリーの RADIUS エリアにも表示されます。
- Add：新規の RADIUS 検査マップを、RADIUS Inspect Maps テーブルの定義リストと Inspect Maps ツリーの RADIUS エリアに追加します。RADIUS マップを新たに設定するには、Inspect Maps ツリーで RADIUS のエントリを選択します。
- Delete：RADIUS Inspect Maps テーブルで選択したアプリケーション検査マップを削除します。Inspect Maps ツリーの RADIUS エリアからも削除されます。

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
•	•	•	•	—

RADIUS Inspect Map Host

RADIUS Inspect Map Host Parameters ペインでは、検査マップのホスト パラメータを設定できます。

フィールド

- Name：事前に設定されている RADIUS アカウンティング マップの名前を示します。

- Description：RADIUS アカウンティング マップの説明を 200 文字以内で入力します。
- Host Parameters：ホストのパラメータを設定できます。
  - Host IP Address：RADIUS メッセージの送信元となるホストの IP アドレスを指定します。
  - Key: (optional)：キーを指定します。
- Add：Host テーブルにホスト エントリを追加します。
- Delete：Host テーブルからホスト エントリを削除します。

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
•	•	•	•	—

RADIUS Inspect Map Other

RADIUS Inspect Map Other Parameters ペインでは、検査マップに追加するパラメータを設定できます。

フィールド

- Name：事前に設定されている RADIUS アカウンティング マップの名前を示します。
- Description：RADIUS アカウンティング マップの説明を 200 文字以内で入力します。
- Other Parameters：追加するパラメータを設定できます。
  - Send response to the originator of the RADIUS message：RADIUS メッセージの送信元ホストにメッセージを返信します。
  - Enforce timeout：ユーザのタイムアウトをイネーブルにします。

    Users Timeout：データベース内のユーザのタイムアウト（hh:mm:ss）。
  - Enable detection of GPRS accounting：GPRS アカウンティングの検出をイネーブルにします。このオプションは、GTP/GPRS ライセンスがイネーブルの場合にのみ使用できます。
  - Validate Attribute：アトリビュート情報です。

    Attribute Number：Accounting Start を受信したときに確認するアトリビュート番号を指定します。

    Add：Attribute テーブルにエントリを追加します。

    Delete：Attribute テーブルからエントリを削除します。

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
•	•	•	•	—