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 ポリシーでは、一貫性と柔軟性を備えた方法で セキュリティ アプライアンス 機能を設定できます。たとえば、サービス ポリシーを使用すると、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ではなく、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。

この章は、次の項で構成されています。

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。説明する内容は次のとおりです。

サポートされる機能

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 接続と UDP 接続の制限およびタイムアウト、TCP シーケンス番号のランダム化
- CSC
- アプリケーション インスペクション
- 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

デフォルトでは、すべてのデフォルト アプリケーション インスペクション トラフィックに一致するポリシーがコンフィギュレーションに含まれ、特定のインスペクションがすべてのインターフェイスのトラフィックに適用されます（グローバル ポリシー）。すべてのインスペクション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。適用できるグローバル ポリシーは 1 つだけなので、グローバル ポリシーを変更する場合は、デフォルトのポリシーを編集するか、デフォルト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します。（インターフェイス ポリシーはグローバル ポリシーに優先します）。

デフォルト ポリシーには、次のアプリケーション インスペクションが含まれます。

- メッセージの最大長 512 バイトに対する DNS インスペクション
- FTP
- H323（H225）
- H323（RAS）
- RSH
- RTSP
- ESMTP
- SQLnet
- Skinny（SCCP）
- SunRPC
- XDMCP
- SIP
- NetBios
- TFTP

機能の方向

アクションは、機能に応じて双方向または単方向にトラフィックに適用されます。双方向に適用される機能の場合、トラフィックが両方向のクラス マップと一致した場合に、ポリシー マップを適用するインターフェイスを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です。単一インターフェイスに適用する場合に通常双方向の機能は、グローバルに適用される場合、各インターフェイスの入力にのみ適用されます。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、ポリシーは両方向に適用され、この場合の双方向は冗長になります。

たとえば、QoS プライオリティ キューのような単方向に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を出るトラフィックだけが影響を受けます。各機能の方向については、表 23-1 を参照してください。

表 23-1　機能の方向

機能	単一インターフェイスでの方向	グローバルでの方向
TCP 正規化、TCP 接続と UDP 接続の制限およびタイムアウト、TCP シーケンス番号のランダム化	双方向	入力
CSC	双方向	入力
アプリケーション インスペクション	双方向	入力
IPS	双方向	入力
QoS 入力ポリシング	入力	入力
QoS 出力ポリシング	出力	出力
QoS プライオリティ キュー	出力	出力

複数のサービス 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 インスペクションがイネーブルの場合は ICMP）の場合、サービス ポリシーはトラフィック フローに対して作用し、個々のパケットに限定されません。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に一致する既存の接続の一部である場合、そのトラフィック フローを別のインターフェイスのポリシーにある同じ機能と照合することはできません。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と一致するときに、HTTP インスペクション用の外部インターフェイスに別のポリシーがある場合、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 トラフィックが外部インターフェイスの入力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 インスペクションをイネーブルにしない場合の ICMP のように、フローとして扱われないトラフィックの場合は、リターン トラフィックを戻り側のインターフェイスの別のポリシー マップと照合できます。たとえば、内部および外部のインターフェイスで IPS 検査を設定し、内部ポリシーでは仮想センサー 1、外部ポリシーでは仮想センサー 2 を使用している場合、非ステートフル ping は仮想センサー 1 の発信側と照合するだけでなく、仮想センサー 2 の着信側とも照合します。

ルール内の複数の機能アクションが適用される順序

1 つの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 接続と UDP 接続の制限およびタイムアウト、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）を実行したり、TCP ペイロード（FTP インスペクション）を変更したりするときは、TCP ノーマライザはデュアル モードで動作します。その場合、サービスを変更するプロキシやペイロードの前後で適用されます。

- CSC
- アプリケーション インスペクション
- 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] 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.** （任意）[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 インスペクションのサービス 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、「デフォルトのグローバル ポリシー」（P.23-2）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（任意）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]：このクラスは、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 ポートのリストについては、「デフォルトの検査ポリシー」（P.24-3）を参照してください。セキュリティ アプライアンス には、デフォルトのインスペクション トラフィックに一致して、すべてのインターフェイス上のトラフィックに共通検査を適用するデフォルト グローバル ポリシーが含まれます。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 アプライアンスがトランスペアレント 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 つだけ指定できます。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]：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]：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、「サービス ポリシー ルールの順序の管理」（P.23-11）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。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だけ表示され、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. （任意）[Description] フィールドに説明を入力します。

f. （任意）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. （任意）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. （任意）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、「時間範囲の設定」（P.8-15）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、「[Add IPSec Remote Access Connection] および [Add SSL VPN Access Connection]」（P.32-68）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。固有の IP 宛先アドレスに向かうトラフィックは、すべてフローと見なされます。

- [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] : RTP ポート範囲を 2000 ～ 65534 の間で入力します。範囲内の最大ポート数は、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 インスペクションの設定」
- 「接続の設定」（P.27-6）
- 「[QoS] タブのフィールド情報」（P.28-2）
- 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。この項では、次のトピックについて取り上げます。

- 「RADIUS アカウンティング インスペクションの概要」（P.23-8）
- 「管理トラフィックのサービス ポリシー ルールの設定」（P.23-8）

RADIUS アカウンティング インスペクションの概要

よく知られている問題の 1 つに GPRS ネットワークでの過剰請求攻撃があります。過剰請求攻撃では、利用していないサービスについて料金を請求されるため、ユーザが怒りや不満を感じるおそれがあります。この場合、悪意のある攻撃者は、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、攻撃者のサーバはパケットの送信を続けます。このパケットは GGSN によってドロップされますが、サーバからの接続はアクティブなままです。攻撃者に割り当てられていた IP アドレスが解放され、正規ユーザに再割り当てされるので、正規ユーザは、攻撃者が利用するサービスの分まで請求されることになります。

RADIUS アカウンティング インスペクションでは、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 アカウンティングの機能を正しく設定しておくと、セキュリティ アプライアンスは、RADIUS アカウンティング要求の開始メッセージと終了メッセージに含まれる Framed IP 属性との照合結果に基づいて接続を切断します。終了メッセージの Framed IP 属性の IP アドレスが一致している場合、セキュリティ アプライアンスは、一致する IP アドレスを持つ送信元との接続をすべて検索します。

セキュリティ アプライアンスでメッセージを検証できるように、RADIUS サーバとの事前共有秘密キーを設定することもできます。事前共有秘密キーを設定しないと、セキュリティ アプライアンスは、メッセージの送信元を検証する必要がなく、その IP アドレスが、RADIUS メッセージの送信を許可されているアドレスの 1 つかどうかだけをチェックします。

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. （任意）[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 インスペクションのサービス 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、「デフォルトのグローバル ポリシー」（P.23-2）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（任意）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 アプライアンスがトランスペアレント 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 つだけ指定できます。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] : 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、「サービス ポリシー ルールの順序の管理」（P.23-11）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.（任意）[Description] フィールドに説明を入力します。

  f.（任意）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.（任意）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. （任意）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、「時間範囲の設定」（P.8-15）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 インスペクションを設定するには、[RADIUS Accounting Map] ドロップダウン リストからインスペクション 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、「RADIUS アカウンティング フィールドの説明」（P.23-12）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]：ホストごとの初期接続の最大数を 65,536 までの範囲で指定します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。この制限により、TCP 代行受信機能がイネーブルになります。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 代行受信は、TCP SYN パケットを使用してインターフェイスをフラッディングすることによる DoS 攻撃から内部システムを保護します。初期接続制限を超えると、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に送信される 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。検証プロセス中に SYN クッキーが使用され、ドロップされる有効なトラフィックの数が最小限に抑えられます。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 つだけ照合できます。
- 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 インスペクション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 インスペクションのルールを照合し、アプリケーション インスペクション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。

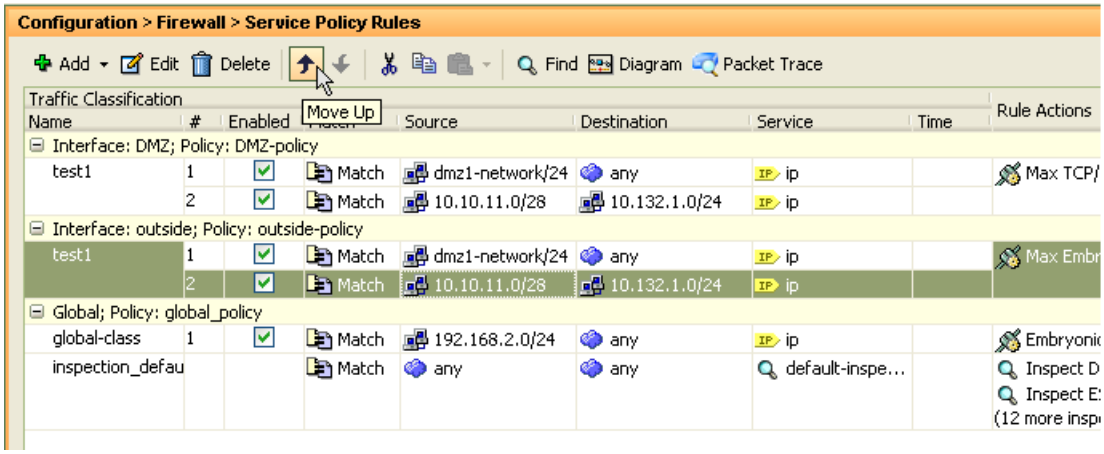
ルールに複数の ACE が組み込まれたアクセス リストが含まれる場合は、ACE の順序もパケット フローに影響します。FWSM は、リストのエントリの順序に従って、各 ACE に対してパケットをテストします。一致が見つかると、ACE はそれ以上チェックされません。たとえば、アクセス リストの先頭にすべてのトラフィックを明示的に許可する ACE を作成した場合、残りのステートメントはチェックされません。

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。説明する内容は次のとおりです。

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

次の表は、この機能を使用できるモードを示したものです。

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]：事前に設定されている 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属性番号を指定します。
  - [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

次の表は、この機能を使用できるモードを示したものです。

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 インスペクション マップ

[RADIUS] ペインでは、事前に設定された RADIUS アプリケーション インスペクション 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 インスペクション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]：インスペクション マップの名前を 40 文字以内で入力します。
- [Description]：インスペクション 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 インスペクション マップを一覧表示するテーブルです。定義されているインスペクション 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 インスペクション 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] 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 インスペクション 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

次の表は、この機能を使用できるモードを示したものです。

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 インスペクション マップ（ホスト）

[RADIUS Inspect Map Host Parameters] ペインでは、インスペクション 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

次の表は、この機能を使用できるモードを示したものです。

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 インスペクション マップ（その他）

[RADIUS Inspect Map Other Parameters] ペインでは、インスペクション 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だけ使用できます。
  - [Validate Attribute]：属性情報です。

    [Attribute Number]：「Accounting Start」を受信したときに確認する属性番号を指定します。

    [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

次の表は、この機能を使用できるモードを示したものです。

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
•	•	•	•	—