CHAPTER 20

サービス ルール

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 ルールでは、特定の種類のアプリケーション検査を、FWSM が受信するさまざまなタイプのトラフィックに適用する方法を定義します。定義により、特定のルールを 1 つのインターフェイスに、またはすべてのインターフェイスに対してグローバルに適用します。

ここでは、次の項目について説明します。

サービス ルール設定の一般的な手順

ASDM では、サービス ルール設定の順序が CLI とは少し異なります。ASDM にサービス ルールを設定するには、一般的に次の 3 つの手順に従って行います。

1. ポリシーを適用するインターフェイスを決定し、ポリシー名を指定します。
2. トラフィック フローを定義する基準を特定します。
3. 指定したトラフィック フローに適用するサービスを特定します。

インターフェイスごとに適用できるポリシーは 1 つだけですが、これに加えてグローバル ポリシーがすべてのインターフェイスに対して適用されます。複数のエントリ（ACE）を持つ ACL を使用する場合を除き、各ポリシーには、トラフィック選択に使用する基準が 1 つ含まれています。

サービス 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　**Security Policy** ペインで **Service Policy Rules** をクリックし、次に **Add** をクリックします。

Add Service Policy Rule Wizard - Service Policy 画面が表示されます。

ステップ 2　サービス ポリシーを作成します。

特定のインターフェイスのセキュリティ ポリシーを作成するには、**Create a service policy and apply to** グループ ボックスで **Interface** オプション ボタンをクリックし、選択リストから使用可能なインターフェイスを選択します。

すべてのインターフェイスに適用するグローバル セキュリティ ポリシーを作成するには、**Create a service policy and apply to** グループ ボックスで **Global** オプション ボタンをクリックします。

ステップ 3　**Policy Name** ボックスに最大 40 文字の名前を入力し、**Next** をクリックします。

Add Service Policy Rule Wizard - Traffic Classification Criteria 画面が表示されます。

ステップ 4　ポリシー ルールを適用するトラフィックを選択する基準を選択します。

Traffic match criteria グループ ボックスにある個々の基準の詳細については、**Add/Edit Security Policy Rules** ウィザードの **Traffic Criteria** ダイアログボックスのオンライン ヘルプを参照してください。

トラフィック フローの定義に複数の基準を使用するには、**Source and destination IP address (uses ACL)** ボタンをクリックします。

ステップ 5　トラフィックに照合する基準を定義したら、**Next** をクリックします。

Add Service Policy Rule Wizard - Rule Actions 画面が表示されます。

ステップ 6　次のタブのいずれかを使用して、指定したトラフィック フローに適用するルール アクションを 1 つ以上定義します。

- **Protocol Inspection**
- **Connection Settings**

ステップ 7　**Finish** をクリックします。

Security Policy ペインの **Service Policy Rules** テーブルに、新しいサービス ポリシーが表示されます。

Service Policy Rules

一部のアプリケーションは、FWSM による特殊な処理を必要としており、この処理のための固有のアプリケーション検査エンジンが用意されています。特別なアプリケーション検査エンジンを必要とするのは、ユーザのデータ パケット内に IP アドレッシング情報を埋め込むか、またはダイナミックに割り当てられたポートでセカンダリ チャネルを開くアプリケーションです。アプリケーション検査は、多くのプロトコルではデフォルトでイネーブルになっていますが、それ以外のプロトコルではディセーブルになっています。多くの場合、アプリケーション検査でトラフィックをリッスンするポートを変更することができます。

アプリケーション検査エンジンは、埋め込まれたアドレッシング情報の場所を特定する NAT と連動します。これによって NAT では、それらの埋め込まれたアドレスを変換したり、変換の影響を受けるチェックサムやその他のフィールドをアップデートしたりできます。

サービス ポリシー ルールでは、特定の種類のアプリケーション検査を、FWSM が受信するさまざまなタイプのトラフィックに適用する方法を定義します。定義により、特定のルールを 1 つのインターフェイスに、またはすべてのインターフェイスに対してグローバルに適用します。

トラフィック照合基準を使用して、アプリケーション検査を適用するトラフィックのセットを定義します。たとえば、ポートの値が 23 の TCP トラフィックは Telnet トラフィック クラスに分類できます。トラフィック クラスを使用して、変更が許可されているプロトコルの場合に、アプリケーション検査で使用するデフォルト ポートを変更できます。

1 つのインターフェイスに複数のトラフィック照合基準を割り当てることができますが、パケットは特定のサービス ポリシー ルール内の最初の基準にのみ一致します。

（注）　**Service Policy** > **Access Rules** ペインのテーブルにあるアクセスリスト ベースのルールを検索するには、メニューバーの Search オプションを使用します。検索しているテキストがアクセスリストに含まれていれば、このオプションを使用してルールを検索できます。

フィールド

- **Add**：新しいサービス ポリシー ルールを追加します。ドロップダウン リストから、追加するルールのタイプを選択します。
- **Edit**：サービス ポリシー ルールを編集します。
- **Delete**：サービス ポリシー ルールを削除します。
- Move Up：ルールを上に移動します。ルールは、このテーブルに表示される順序で評価されるため、重複するルールがあると順序によって評価が異なります。
- Move Down：ルールを下に移動します。
- Cut：ルールを切り取ります。
- Copy：ルールのパラメータをコピーし、Paste ボタンを使用して、同じパラメータを持つ新しいルールを開始できます。

- Paste : コピーまたは切り取られたルールのパラメータがあらかじめ入力された状態で、Add/Edit Rule ダイアログボックスを開きます。ダイアログボックスで何らかの修正を行い、ルールをテーブルに追加することができます。Paste ボタンをクリックすると、選択したルールの上にルールが追加されます。Paste ドロップダウン リストから Paste After 項目を選択すると、選択したルールの後にルールが追加されます。
- Find : 表示をフィルタリングして、一致するルールのみを表示します。**Find** をクリックすると、Filter フィールドが開きます。Filter フィールドを非表示にするには、もう一度 **Find** をクリックします。
  - Filter : フィルタリングする基準を、Interface、Source、Destination、Service、または Rule Query のいずれかから選択します。ルール クエリーは複数の基準の集合であり、保存して繰り返し使用できます。
  - Filter : Interface タイプの場合は、このフィールドがドロップダウン リストになります。インターフェイス名または **All Interfaces** を選択できます。Rule Query タイプの場合、ドロップダウン リストにはすべての定義済みルール クエリーが表示されます。Source タイプと Destination タイプの場合には、IP アドレスを指定できます。アドレスを手動で入力するか、または **...** ボタンをクリックして Browse Address ダイアログボックスを開き、アドレスを参照します。Service タイプには、TCP、UDP、TCP-UDP、ICMP、または IP プロトコル タイプを指定できます。プロトコル タイプを手動で入力するか、または **...** ボタンをクリックして Browse Service Groups ダイアログボックスを開き、プロトコル タイプを参照します。
  - Filter : フィルタリングを実行します。
  - Clear : Filter フィールドをクリアします。
  - Rule Query : Rule Queries ダイアログボックスを開き、名前付きルール クエリーを管理できます。
- Show Rule Flow Diagram : ルール テーブルの下に Rule Flow Diagram 領域を表示します。この図には、ネットワーク、トラフィックのタイプ、インターフェイス名、フロー方向、およびアクションが表示されます。
- Packet Trace : 選択したルールの特性を示すパラメータがあらかじめ入力された状態で Packet Tracer ツールが開きます。

次に、Service Policy Rules テーブルのカラムの概要を説明します。これらのカラムの内容は、テーブル セルをダブルクリックすると編集できます。カラム ヘッダーをダブルクリックすると、選択したカラムをソート キーとして、テーブルの内容がアルファベットの昇順で並べ替えられます。ルールを右クリックすると、上のボタンで示されるオプションすべてとともに、Insert 項目と Insert After 項目が表示されます。これらの項目により、選択したルールの前（Insert）または後（Insert After）に新しいルールを挿入します。

- **Name** : ルールの名前を示します。
- **No :** ルールの評価順序を示します。
- **Enabled :** ルールがイネーブルになっているか、またはディセーブルになっているかを示します。
- **Match :** トラフィックを含める（一致する）か除外する（一致しない）ために基準を使用するかどうかを示します。
- **Source :** Destination カラムのリストにある IP アドレス宛てにトラフィックが送信されるときのサービス ポリシーに従う IP アドレスを一覧表示します。
- **Destination :** Source カラムのリストにある IP アドレスからトラフィックが送信されるときのサービス ポリシーに従う IP アドレスを一覧表示します。
- **Service :** ルールで指定されるサービスまたはプロトコルを表示します。
- **Time :** ルールを適用する時間範囲が表示されます。
- Rule Actions : ルールで適用されるアクションを表示します。
- **Description :** ルールの追加時に入力した説明です。

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
•	•	•	•	—

Service Policy

Service Policy ダイアログボックスでは、新しいサービス ポリシー ルールを追加したり、そのルールを特定のインターフェイスに適用したり、そのルールをすべてのインターフェイスに対してグローバルに適用したりすることができます。

フィールド

- Create a Service Policy and Apply to
  - Interface : ルールを特定のインターフェイスに適用します。アクセスリストを使用し、送信元または宛先 IP アドレスに基づいてトラフィックを照合する場合は、このフィールドを選択する必要があります。
  - Interface：ルールを適用するインターフェイスを指定します。
  - Policy Name：インターフェイス サービス ポリシーの名前を指定します。
  - Description：ポリシーの説明をテキストで入力します。
  - Global - applies to all interfaces：ルールをすべてのインターフェイスに適用します。アクセスリストを使用し、送信元または宛先 IP アドレスに基づいてトラフィックを照合する場合は、このフィールドを一緒に選択できません。
  - Policy Name：グローバル サービス ポリシーの名前を指定します。グローバル サービス ポリシーは、1 つしか適用できません。また、名前を変更することはできません。
  - Description：ポリシーの説明をテキストで入力します。

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
•	•	•	•	—

Edit Service Policy

Edit Service Policy ダイアログボックスでは、選択したサービス ポリシーの説明を変更できます。

フィールド

- Description：サービス ポリシーの説明をテキストで入力します。

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
•	•	•	•	—

Traffic Classification Criteria

Edit Service Policy Rule 画面の Traffic Classification タブでは、セキュリティ ポリシー ルールを適用するトラフィックの照合の際に使用する基準を指定できます。

フィールド

- Name：トラフィック クラスの名前を特定します。
- Description (optional)：新しいトラフィック クラスの説明をテキストで入力します。
- Traffic match criteria：
  - Default Inspection Traffic：デフォルトの検査トラフィック ポリシーで指定された基準を使用します。
  - Source and Destination IP Address (uses ACL) : ACL を使用し、送信元と宛先 IP アドレスに基づいてトラフィックを照合します。このフィールドは、インターフェイス サービス ポリシーを使用して特定のインターフェイスにルールを適用する場合にのみ選択できます。
  - TCP or UDP Destination Port : TCP または UDP 宛先ポートに基づいてトラフィックを照合します。
  - RTP Range：RTP ポートの範囲に基づいてトラフィックを照合します。
  - IP DiffServ CodePoints (DSCP)：QoS の Differentiated Services モデルに基づいてトラフィックを照合します。
  - IP Precedence：QoS の IP precedence モデルに基づいてトラフィックを照合します。
  - Any traffic：トラフィック タイプに関係なくすべてのトラフィックを照合します。
- Add rule to existing traffic class : リストで選択した既存のトラフィック クラスにルールを追加します。
- Use class-default as the traffic class：トラフィックが他のトラフィック クラスのどれとも一致しない場合は、class-default トラフィック クラスを使用するように指定します。

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
•	•	•	•	—

Default Inspections

Default Inspections ダイアログボックスには、Traffic Classification Criteria ダイアログボックスで Default Inspection Traffic 基準を選択する場合に使用される、デフォルトのポート割り当てがリストで表示されます。

- Service：アプリケーション検査エンジンのタイプをリストで表示します。
- Protocol：トランスポート プロトコルとして、TCP と UDP のどちらをアプリケーション検査で使用するかを特定します。
- Port：デフォルトの検査トラフィック基準で使用されるポート番号を特定します。

デフォルトの検査トラフィック基準の使用

fixup コマンドは、アプリケーション検査に簡易でグローバルなポリシーを提供しました。モジュラ ポリシー フレームワークには、さらにきめ細かなトラフィックの検査方法が用意されています。モジュラ ポリシー フレームワークでは、特定のアプリケーション検査で使用するトラフィックを選択することができ、これによって、FWSM のパフォーマンスを向上させることができます。パフォーマンスが向上する理由は、アプリケーション検査エンジンが限定された量のトラフィックのみを検査するからです。

デフォルト ポートでのアプリケーション検査のイネーブル化を簡単にするため、デフォルトの検査トラフィック基準を使用します。デフォルトの検査トラフィック基準を指定すると、FWSM は、ウェルノウン ポートのアプリケーション検査で使用するトラフィックをプロトコルごとに選択します。表 20-1 に、プロトコルごとのデフォルト ポートの割り当てを示します。

表 20-1　デフォルト ポートの割り当て

プロトコル名	プロトコル	セキュア ポート	宛先ポート
ctiqbe	tcp	該当なし	2748
dcerpc	tcp	該当なし	135
dns	udp	53	53
esmtp/smtp	tcp	該当なし	25
ftp	tcp	該当なし	21
gtp	udp	2123,3386	2123,3386
h323 h225	tcp	該当なし	1720
h323 ras	udp	該当なし	1718-1719
http	tcp	該当なし	80
icmp	icmp	該当なし	該当なし
ils	tcp	該当なし	389
mgcp	udp	2427,2727	2427,2727
netbios	udp	137-138	該当なし
pptp	tcp	1723	1723
rsh	tcp	該当なし	514
rtsp	tcp	該当なし	554
sip	tcp、udp	該当なし	5060
skinny	tcp	該当なし	2000
sqlnet	tcp	該当なし	1521
sunrpc	udp	111	111
tftp	udp	該当なし	69

表 20-1　デフォルト ポートの割り当て（続き）

プロトコル名	プロトコル	セキュア ポート	宛先ポート
waas	該当なし	該当なし	該当なし
xdmcp	udp	177	177

デフォルトの検査トラフィック基準を選択する場合は、Rule Actions 画面の Protocol Inspection タブで各プロトコルをイネーブルにすることができます。プロトコルは、そのプロトコルのデフォルト ポートでイネーブルにされます。検査対象を特定のフローに限定するには、Source and destination IP address (uses ACL) ボタンを使用し、Service Policy Rule 画面から Source Host/Network または Destination Host/Network などの具体的な基準を選択します。

（注）　デフォルトの検査トラフィック基準は、Protocol and Service グループ ボックスのどのポート設定よりも優先されます。つまり、デフォルトの検査トラフィック基準を使用している間は、どのプロトコルの場合にもデフォルト ポートの割り当てを一切変更できません。

inspection_default セキュリティ ポリシーは、デフォルトの検査トラフィック基準を使用したアプリケーション検査を可能にする事前設定済みのグローバル ポリシーです。このグローバル ポリシーは、FWSM の工場出荷時のデフォルト コンフィギュレーションでイネーブルに設定されます。

（注）　デフォルトの検査トラフィック基準をトラフィック照合基準に指定する場合は、指定されたインターフェイスのセキュリティ ポリシーで検査ルール アクションのみを適用できます。Connection Settings タブのアクションを適用することはできません。

アプリケーション検査のデフォルト ポートの変更

デフォルトの検査トラフィック基準は、Protocol and Service グループ ボックスのどのポート設定よりも優先されます。つまり、デフォルトの検査トラフィック基準を使用している間は、どのプロトコルの場合にもデフォルト ポートの割り当てを一切変更できません。

任意のプロトコルのデフォルト ポート割り当てを変更するには、各検査エンジンを手動で設定してイネーブルにする必要があります。

モジュラ ポリシー フレームワークを使用してプロトコルのデフォルト ポート割り当てを変更するには、次の手順を実行します。

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

Add Service Policy Rule Wizard - Service Policy 画面が表示されます。

ステップ 2　サービス ポリシーを作成します。

特定のインターフェイスのセキュリティ ポリシーを作成するには、**Create a service policy and apply to** グループ ボックスで **Interface** オプション ボタンをクリックし、選択リストから使用可能なインターフェイスを選択します。

すべてのインターフェイスに適用するグローバル セキュリティ ポリシーを作成するには、**Create a service policy and apply to** グループ ボックスで **Global** オプション ボタンをクリックします。

ステップ 3　**Policy Name** ボックスに最大 40 文字の名前を入力し、**Next** をクリックします。

Add Service Policy Rule Wizard - Traffic Classification Criteria 画面が表示されます。

ステップ 4　**Source and destination IP address (uses ACL)** ボタンをクリックします。

ステップ 5　**Protocol and Service** グループ ボックスで、プロトコルの **Source Port** および **Destination Port** を選択し、**Next** をクリックします。

Add Service Policy Rule Wizard - Rule Actions 画面が表示されます。

ステップ 6　イネーブルにするプロトコルのチェックボックスをオンにし、**Finish** をクリックします。

Security Policy ペインの **Service Policy Rules** テーブルに、新しいサービス ポリシーが表示されます。

ステップ 7　別の検査エンジンをイネーブルにするには、サービス ポリシーを選択して **Add** をクリックします。

Add Service Policy Rule Wizard - Service Policy 画面が表示されます。

ステップ 8　**Next** をクリックします。

Add Service Policy Rule Wizard - Traffic Classification Criteria 画面が表示されます。

ステップ 9　**Create a new traffic class** をクリックし、必要に応じてトラフィック クラスの名前を変更します。

デフォルトでは、新しいクラスを追加するたびに各トラフィック クラスの名前の終わりにある番号が増分されます。

ステップ 10　**Source and destination IP address (uses ACL)** をクリックします。

ステップ 11　**Traffic Match** タブをクリックします。

ステップ 12　**Protocol and Service** グループ ボックスのプロトコル用に 2 番目のポート番号を選択し、**OK** をクリックします。

Security Policy ペインの **Service Policy Rules** テーブルに新しいアクセス コントロール エントリが表示されます。

複数ポートによるアプリケーション検査の設定

モジュラ ポリシー フレームワークを使用して複数のポートを使用するプロトコルのデフォルト ポート割り当てを変更するには、次の手順を実行します。

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

Add Service Policy Rule Wizard - Service Policy 画面が表示されます。

ステップ 2　サービス ポリシーを作成します。

特定のインターフェイスのセキュリティ ポリシーを作成するには、**Create a service policy and apply to** グループ ボックスで **Interface** オプション ボタンをクリックし、選択リストから使用可能なインターフェイスを選択します。

すべてのインターフェイスに適用するグローバル セキュリティ ポリシーを作成するには、**Create a service policy and apply to** グループ ボックスで **Global** オプション ボタンをクリックします。

ステップ 3　**Policy Name** ボックスに最大 40 文字の名前を入力し、**Next** をクリックします。

Add Service Policy Rule Wizard - Traffic Classification Criteria 画面が表示されます。

ステップ 4　**Source and destination IP address (uses ACL)** ボタンをクリックします。

ステップ 5　**Protocol and Service** グループ ボックスのプロトコル用に最初のポート番号を選択し、**Next** をクリックします。

Add Service Policy Rule Wizard - Rule Actions 画面が表示されます。

ステップ 6　次のタブのいずれかを使用して、指定したトラフィック フローに適用するルール アクションを定義します。

- **Protocol Inspection**
- **Connection Settings**

ステップ 7　**Finish** をクリックします。

Security Policy ペインの **Service Policy Rules** テーブルに、新しいサービス ポリシーが表示されます。

ステップ 8　Service Policy Rules テーブルでセキュリティ ポリシーを右クリックします。

ステップ 9　表示されるポップアップ メニューで、**Insert After** を選択します。

Insert Service Policy Rule After 画面が表示されます。

ステップ 10　**Traffic Match** タブをクリックします。

ステップ 11　**Protocol and Service** グループ ボックスのプロトコル用に 2 番目のポート番号を選択し、**OK** をクリックします。

Security Policy ペインの **Service Policy Rules** テーブルに新しいアクセス コントロール エントリが表示されます。

Source and Destination Address（他のコンテキストでの名称は「ACL」）

（このダイアログボックスは、サービス ポリシー ルールを編集する場合は **ACL** と呼ばれます）

このダイアログボックスでは、送信側または受信側ホストの IP アドレスまたは TCP/UDP ポートに基づいて、サービス ポリシー ルールを適用するトラフィックを特定できます。また、このダイアログボックスを使用して、ポリシー ルールを有効にする **Time Range** を選択することもできます。

フィールド

- Select an action：このダイアログボックスで指定した基準にトラフィックが一致する必要がある、またはその基準に一致しないようにするかを指定できます。
- Time Range
  - Time Range：ポリシー ルールを有効にする時間範囲を選択できます。
  - New：Add Time Range ダイアログボックスにアクセスできます。詳細については、「Add/Edit Time Range」を参照してください。
- Source Host/Network x
  - IP Address：トラフィックの送信元を IP アドレスによって識別するように指定します。このボタンを選択すると、グループ ボックス内に、Interface リスト、IP address ボックス、. . . ボタン、Mask リストが表示されます。
  - Name：トラフィックの送信元をインターフェイス名によって識別するように指定します。このボタンを選択すると、グループ ボックス内に、Name リストが表示されます。
  - Group：トラフィックの送信元をオブジェクト グループによって識別するように指定します。このボタンを選択すると、グループ ボックス内に、Interface リストと Group リストが表示されます。
  - Interface：トラフィックの送信元がオンになっているインターフェイスの名前を指定します。リストは、IP Address ボタンか Group ボタンが選択されている場合にのみ表示されます。
  - IP address：トラフィックの送信元を識別するために使用する IP アドレスを指定します。このボックスは、IP Address ボタンが選択されている場合にのみ表示されます。
  - . . .：Select host/network ダイアログボックスにアクセスできます。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。このボタンは、IP Address ボタンが選択されている場合にのみ表示されます。
  - Mask：IP address ボックスに入力したアドレスのサブネット マスクを指定します。このボックスは、IP Address ボタンが選択されている場合にのみ表示されます。
  - Name：トラフィックの送信元がオンになっているインターフェイスの名前を指定します。このリストは、Name ボタンが選択されている場合にのみ表示されます。
  - Group：トラフィックの送信元が属しているオブジェクト グループを指定します。リストの項目は、Hosts/Networks ペインで制御されます。このペインの詳細については、「ネットワーク オブジェクトの概要」を参照してください。このグループ リストは、Group ボタンが選択されている場合にのみ表示されます。
- Destination Host/Network
  - IP Address：トラフィックの宛先を IP アドレスによって識別するように指定します。このボタンを選択すると、グループ ボックス内に、Interface リスト、IP address ボックス、. . . ボタン、Mask リストが表示されます。
  - Name：トラフィックの宛先をインターフェイス名によって識別するように指定します。このボタンを選択すると、グループ ボックス内に、Name リストが表示されます。
  - Group：トラフィックの宛先をオブジェクト グループによって識別するように指定します。このボタンを選択すると、グループ ボックス内に、Interface リストと Group リストが表示されます。
  - Interface：トラフィックの宛先がオンになっているインターフェイスの名前を指定します。このリストは IP Address ボタンまたは Group ボタンが選択されている場合にのみ表示されます。

  - IP address : トラフィックの宛先を識別するために使用する IP アドレスを指定します。このボックスは、IP Address ボタンが選択されている場合にのみ表示されます。
  - . . . : Select host/network ダイアログボックスにアクセスできます。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。このボタンは、IP Address ボタンが選択されている場合にのみ表示されます。
  - Mask : IP address ボックスに入力したアドレスのサブネット マスクを指定します。このボックスは、IP Address ボタンが選択されている場合にのみ表示されます。
  - Name : トラフィックの宛先がオンになっているインターフェイスの名前を指定します。このリストは、Name ボタンが選択されている場合にのみ表示されます。
  - Group : トラフィックの宛先が属しているオブジェクト グループを指定します。リストの項目は Hosts/Networks ペインで制御されます。このペインの詳細については、「ネットワーク オブジェクトの概要」を参照してください。このグループ リストは、Group ボタンが選択されている場合にのみ表示されます。

- Rule Flow Diagram : FWSM によって転送されるトラフィックに対する、特定のフィルタリング アクションの適用方法をグラフィカルに表現します。
- Protocol and Service
  - TCP : TCP プロトコルまたはサービスに基づいてトラフィックを照合します。
  - UDP : UDP プロトコルまたはサービスに基づいてトラフィックを照合します。
  - ICMP : ICMP プロトコルの値に基づいてトラフィックを照合します。
  - IP : IP プロトコルの値に基づいてトラフィックを照合します。
  - Manage Service Groups : Manage Service Groups ダイアログボックスを表示します。このダイアログボックスでは、サービス グループを作成および編集できます。このボタンは、TCP ボタンが選択されている場合にのみ使用できます。
  - Source Port : TCP または UDP のオプション ボタンが選択されている場合にのみ表示されます。

    Service : 送信元ポートの値に基づいてトラフィックを照合します。

    Operator : 照合する 1 つのポート、またはポートの範囲を特定するかどうかを指定します。リストから、=（と等しい）、not=（と等しくない）、>（より大きい）、<（より小さい）を選択すると、. . . ボタンが表示されます。このボタンにより、特定の名前付きポートを選択できます。リストから range を選択すると、2 つのボックスが表示されます。それらのボックスに、範囲の開始ポートと終了ポートを入力できます。

    ... : Service ダイアログボックスを表示します。このダイアログボックスでは、照合する TCP または UDP ポートの名前付きの値を選択できます。

    Service Group : 送信元サービス グループに基づいてトラフィックを照合します。リストの項目を制御するには、**Manage Service Groups** ボタンを使用します。
  - Destination Port : TCP または UDP のオプション ボタンが選択されている場合にのみ表示されます。

    Service : 宛先ポートの値に基づいてトラフィックを照合します。

    Operator : 照合する 1 つのポート、またはポートの範囲を特定するかどうかを指定します。リストから、=（と等しい）、not=（と等しくない）、>（より大きい）、<（より小さい）を選択すると、. . . ボタンが表示されます。このボタンにより、特定の名前付きポートを選択できます。リストから range を選択すると、2 つのボックスが表示されます。それらのボックスに、範囲の開始ポートと終了ポートを入力できます。

    ... : Service ダイアログボックスを表示します。このダイアログボックスでは、照合する TCP または UDP ポートの名前付きの値を選択できます。

    Service Group : 宛先サービス グループに基づいてトラフィックを照合します。リストの項目を制御するには、Manage Service Groups ボタンを使用します。
  - ICMP Type : ICMP オプション ボタンが選択されている場合にのみ表示されます。

    ICMP type : トラフィックの ICMP タイプを入力できます。

    ... : Service ダイアログボックスを表示します。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 ICMP タイプを選択できます。

— IP Protocol：IP オプション ボタンが選択されている場合にのみ表示されます。

IP protocol：トラフィックの IP プロトコルを入力できます。

...：Service ダイアログボックスを表示します。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 IP プロトコルを選択できます。

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
•	•	•	•	—

Destination Port

Destination Port ダイアログボックスは、Traffic Match Criteria ダイアログボックスで TCP or UDP destination port を選択する場合、またはサービス ポリシー ルールの編集時に対応するタブをクリックする場合に表示されます。このダイアログボックスでは、TCP または UDP の宛先ポートに基づいて、サービス ポリシー ルールを適用するトラフィックを特定できます。

フィールド

- TCP：宛先で使用される TCP ポートに基づいてトラフィックを照合します。
- UDP：宛先で使用される UDP ポートに基づいてトラフィックを照合します。
- Operator：照合する 1 つのポート、またはポートの範囲を特定するかどうかを指定します。

  リストから =（等号）を選択すると、. . . ボタンが表示されます。このボタンにより、特定の名前付きポートを選択できます。

  リストから range を選択すると、2 つのボックスが表示されます。それらのボックスに、範囲の開始ポートと終了ポートを入力できます。
- ... : Service ダイアログボックスを表示します。このダイアログボックスでは、照合する TCP または UDP ポートの名前付きの値を選択できます。

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
•	•	•	•	—

Rule Actions > Protocol Inspection タブ

Protocol Inspection タブでは、使用可能なさまざまなタイプのアプリケーション検査をイネーブルまたはディセーブルにすることができます。特定のアプリケーション検査タイプの設定を表示または変更するには、**Configure** を選択します。これによって、プロトコルで使用するマップ名を選択できます。マップの設定については、P.6-9 の「検査マップの設定」を参照してください。

フィールド

- CTIQBE：CTIQBE プロトコルでのアプリケーション検査をイネーブルにします。
- DCERPC：DCERPC プロトコルでのアプリケーション検査をイネーブルにします
  - Configure：Configure DCERPC ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- DNS：DNS プロトコルでのアプリケーション検査をイネーブルにします。
  - Configure：Configure DNS ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- ESMTP：ESMTP プロトコルでのアプリケーション検査をイネーブルにします。ESMTP アプリケーション検査は、SMTP アプリケーション検査がディセーブルの場合のみ、イネーブルになります。ESMTP アプリケーション検査は、コントロール プレーン パス処理で行います。したがって、FWSM にある 1 台の汎用プロセッサに対して行います。
- FTP：FTP プロトコルでのアプリケーション検査をイネーブルにします。
  - Configure：Select FTP Map ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- GTP：GTP プロトコルでのアプリケーション検査をイネーブルにします。
  - Configure：Select GTP Map ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。

（注）　GTP 検査は、特別なライセンスがなければ使用できません。

- H323 H225：H323 H225 プロトコルでのアプリケーション検査をイネーブルにします。
  - Configure：Select H.225 Map ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- H323 RAS：H323 RAS プロトコルでのアプリケーション検査をイネーブルにします。
- HTTP：HTTP プロトコルでのアプリケーション検査をイネーブルにします。
  - Configure：Select HTTP Map ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- ICMP：ICMP プロトコルでのアプリケーション検査をイネーブルにします。
- ICMP Error：ICMP Error プロトコルでのアプリケーション検査をイネーブルにします。
- ILS：ILS プロトコルでのアプリケーション検査をイネーブルにします。
- MGCP：MGCP プロトコルでのアプリケーション検査をイネーブルにします。
  - Configure：Select MGCP Map ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- NETBIOS：NetBIOS プロトコルでのアプリケーション検査をイネーブルにします。
- PPTP：PPTP プロトコルでのアプリケーション検査をイネーブルにします。
- RSH：RSH プロトコルでのアプリケーション検査をイネーブルにします。
- RTSP：RTSP プロトコルでのアプリケーション検査をイネーブルにします。
- SIP：SIP プロトコルでのアプリケーション検査をイネーブルにします。

  - Configure：Select SIP Map ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- SKINNY：Skinny プロトコルでのアプリケーション検査をイネーブルにします。
- SMTP：SMTP プロトコルでのアプリケーション検査をイネーブルにします。SMTP アプリケーション検査は、ESMTP アプリケーション検査がディセーブルの場合のみ、イネーブルになります。SMTP アプリケーション検査は、高速パス処理で行います。したがって、FWSM にある 3 台のネットワーク プロセッサのうちの 1 台で行います。
- SNMP：SNMP プロトコルでのアプリケーション検査をイネーブルにします。
  - Configure：Select SNMP Map ダイアログボックスを表示します。このダイアログボックスでは、このプロトコルで使用するマップ名を選択できます。
- SQLNET：SQLNET プロトコルでのアプリケーション検査をイネーブルにします。
- SUNRPC：SunRPC プロトコルでのアプリケーション検査をイネーブルにします。
- TFTP：TFTP プロトコルでのアプリケーション検査をイネーブルにします。
- WAAS: WAAS プロトコルでのアプリケーション検査をイネーブルにします。
- XDMCP：XDMCP プロトコルでのアプリケーション検査をイネーブルにします。

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

- 検査マップの設定（P.6-9）
- 『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』にあるプロトコルごとの **Inspect** コマンド ページ

Configure DCERPC

Select DCERPC Inspect Map ダイアログボックスでは、DCERPC アプリケーション検査のイネーブル化、DCERPC マップの選択と編集、または新しい DCERPC マップの作成を行うことができます。DCERPC マップでは、DCERPC アプリケーション検査の設定値を変更できます。Select DCERPC Map テーブルには、アプリケーション検査をイネーブルにするときに選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- Use the default DCERPC inspection map：DCERPC マップが DCERPC アプリケーション検査へ適用されるのを避けるためには、このボタンをイネーブルにします。
- Select a DCERPC map for fine control over inspection radio：DCERPC マップを DCERPC アプリケーション検査に適用するためには、このボタンをイネーブルにします。このボタンをイネーブルにしてから、事前に定義したマップを選択して適用するか、Add をクリックして新しいマップを定義します。
- Add：Add DCERPC Map 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、新しいアプリケーション検査マップを作成し、使用するコンフィギュレーション設定を定義できます。

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
•	•	•	•	—

Configure DNS

フィールド

Maximum DNS packet length (default 512) : FWSM の通過が許可されている DNS メッセージの最大パケット長を変更します。

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
•	•	•	•	—

Select FTP Map

Select FTP Map ダイアログボックスでは、厳密な FTP アプリケーション検査のイネーブル化、FTP マップの選択と編集、または新しい FTP マップの作成を行うことができます。FTP マップにより、FTP 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値を変更できます。Select FTP Map テーブルには、アプリケーション検査をイネーブルにするときに選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- FTP Strict (prevent web browsers from sending embedded commands in FTP requests) : 厳密な FTP アプリケーション検査をイネーブルにします。これによって FWSM は、埋め込みコマンドが FTP 要求に含まれている場合には接続をドロップします。
- Add : Add DCERPC Map 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、新しいアプリケーション検査マップを作成し、使用するコンフィギュレーション設定を定義できます。

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
•	•	•	•	—

Select GTP Map

Select GTP Map ダイアログボックスでは、GTP アプリケーション検査のイネーブル化、GTP マップの選択と編集、または新しい GTP マップの作成を行うことができます。GTP マップにより、GTP 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値を変更できます。Select GTP Map テーブルには、アプリケーション検査をイネーブルにするときに選択可能な事前に設定されたマップのリストが表示されます。

（注） GTP 検査には、特別なライセンスが必要です。必要なライセンスがないときに FWSM で GTP アプリケーション検査のイネーブル化を試みると、FWSM はエラー メッセージを表示します。

フィールド

- Add：Add GTP Map 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、新しいアプリケーション検査マップを作成し、使用するコンフィギュレーション設定を定義できます。

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
•	•	•	•	—

Select H.225 Map

Select H.225 Map ダイアログボックスでは、厳密な H.225 アプリケーション検査のイネーブル化（アプリケーション ファイアウォールと呼ばれる場合もある）、H.225 マップの選択と編集、または新しい H.225 マップの作成を行うことができます。H.225 マップにより、H.225 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値を変更できます。Select H.225 Map テーブルには、アプリケーション検査をイネーブルにするときに選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- **Add**：Add H.225 Map 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、新しいアプリケーション検査マップを作成し、使用するコンフィギュレーション設定を定義できます。

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
•	•	•	•	—

Select HTTP Map

Select HTTP Map ダイアログボックスでは、厳密な HTTP アプリケーション検査のイネーブル化（アプリケーション ファイアウォールと呼ばれる場合もある）、HTTP マップの選択と編集、または新しい HTTP マップの作成を行うことができます。HTTP マップにより、HTTP 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値を変更できます。Select HTTP Map テーブルには、アプリケーション検査をイネーブルにするときに選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- Add：Add HTTP Map 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、新しいアプリケーション検査マップを作成し、使用するコンフィギュレーション設定を定義できます。

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
•	•	•	•	—

Select MGCP Map

Select MGCP Map ダイアログボックスでは、MGCP アプリケーション検査のイネーブル化、MGCP マップの選択と編集、または新しい MGCP マップの作成を行うことができます。MGCP マップにより、MGCP 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値を変更できます。Select MGCP Map テーブルには、アプリケーション検査をイネーブルにするときに選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- Add：Add MGCP Map 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、新しいアプリケーション検査マップを作成し、使用するコンフィギュレーション設定を定義できます。

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
•	•	•	•	—

Select SIP Map

Select SIP Map ダイアログボックスでは、厳密な SIP アプリケーション検査のイネーブル化（アプリケーション ファイアウォールと呼ばれる場合もある）、SIP マップの選択と編集、または新しい SIP マップの作成を行うことができます。SIP マップでは、SIP アプリケーション検査の設定値を変更できます。Select SIP Map テーブルには、アプリケーション検査をイネーブルにするときに選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- Use the default SIP inspection map：SIP マップが SIP アプリケーション検査へ適用されるのを避けるためには、このボタンをイネーブルにします。
- Select a SIP map for fine control over inspection radio：SIP マップを SIP アプリケーション検査に適用するためには、このボタンをイネーブルにします。このボタンをイネーブルにしてから、事前に定義したマップを選択して適用するか、Add をクリックして新しいマップを定義します。
- Add：Add SIP Map 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、新しいアプリケーション検査マップを作成し、使用するコンフィギュレーション設定を定義できます。

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
•	•	•	•	—

Select SNMP Map

Select SNMP Map ダイアログボックスでは、SNMP アプリケーション検査のイネーブル化、SNMP マップの選択と編集、または新しい SNMP マップの作成を行うことができます。SNMP マップにより、SNMP 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値を変更できます。Select SNMP Map テーブルには、アプリケーション検査をイネーブルにするときに選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- Add：Add SNMP Map 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、新しいアプリケーション検査マップを作成し、使用するコンフィギュレーション設定を定義できます。

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
•	•	•	•	—

TCP ステート バイパスの概要

Rule Actions > Connection Settings タブで TCP State Bypass チェックボックスをオンにすると、TCP ステート バイパスを設定できます。この項では、TCP ステート バイパスの使用方法について説明します。次の項目を取り上げます。

- 別個の FWSM を通過する発信および着信フローの許可（P.20-20）
- サポートされていない機能（P.20-21）
- NAT との互換性（P.20-21）
- 接続タイムアウト（P.20-21）

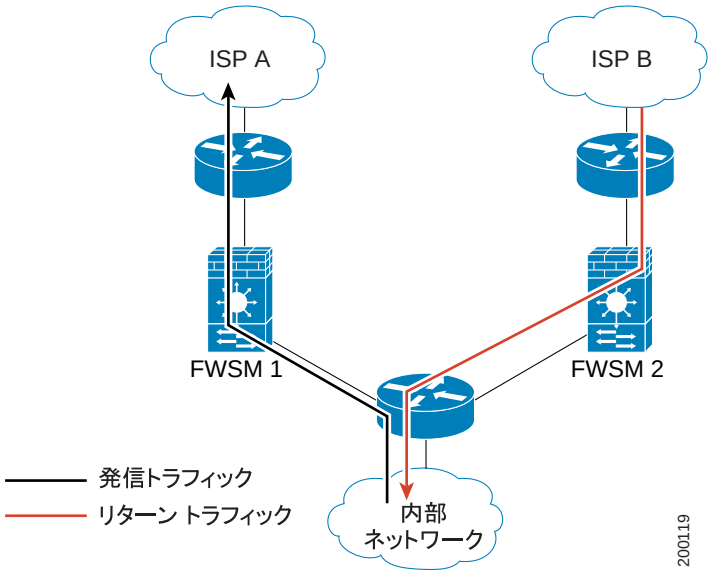
別個の FWSM を通過する発信および着信フローの許可

デフォルトでは、FWSM を通過するすべてのトラフィックは、アダプティブ セキュリティ アルゴリズムによって検査され、セキュリティ ポリシーに基づいて、許可またはドロップされます。FWSM は、各パケットの状態（新規接続か、既存接続か）をチェックし、セッション管理パス（新規接続の SYN パケット）、高速パス（既存接続）、コントロール プレーン パス（高度な検査）のいずれかに割り当てることによって、ファイアウォールのパフォーマンスを最大化します。

高速パスで既存接続を照合する TCP パケットは、セキュリティ ポリシーをすべて再照合しなくても FWSM を通過できます。この機能によって、パフォーマンスが最大化されます。ただし、SYN パケットを使用して高速パスでセッションを確立する方法や、高速パスで発生する照合（TCP シーケンス番号など）は、非対称ルーティング ソリューションの障害になることがあります。接続の発信および着信フローは同じ FWSM を通過する必要があります。

たとえば、新規接続は、FWSM 1 に向かいます。SYN パケットは、セッション管理パスを通過し、接続のエントリが高速パス テーブルに追加されます。この接続の後続のパケットは、FWSM 1 を通過した後で高速パスのエントリを照合し、通過します。ただし、後続のパケットが FWSM 2 へ向かうと、そこにはセッション管理パスを通過した SYN パケットがなく、接続の高速パスのエントリもないため、パケットは、ドロップします。図 20-1 は、発信トラフィックが着信トラフィックと異なる FWSM を通過する非対称ルーティングの例を示しています。

図 20-1　非対称ルーティング



アップストリーム ルータに非対称ルーティングが設定され、トラフィックが 2 つの FWSM を交互に通過する場合は、特定のトラフィックの TCP ステート バイパスを設定できます。TCP ステート バイパスは、高速パスに確立されているセッションの方法を変更し、高速パスの照合をディセーブルにします。この機能は、UDP 接続を処理するように TCP トラフィックを処理します。指定されたネットワークに照合する non-SYN パケットが FWSM に入り、高速パスのエントリがない場合、パケットは、高速パスに接続を確立するためにセッション管理パスを通過します。高速パスに入ると、トラフィックは高速パス照合をバイパスします。

サポートされていない機能

TCP ステート バイパスを使用する場合、次の機能はサポートされていません。

- アプリケーション検査 : アプリケーション検査は、着信および発信トラフィックが同じ FWSM を通過することを要求します。したがって、アプリケーション検査は、TCP ステート バイパスではサポートされていません。
- AAA 認証セッション : 1 つの FWSM を認証する場合、別の FWSM を経由するトラフィックは、ユーザがそれを認証していないため拒否されます。

NAT との互換性

変換セッションが各 FWSM に別個に確立されるため、スタティック NAT を TCP ステート バイパス トラフィックの両方の FWSM に必ず設定してください。ダイナミック NAT を使用する場合は、FWSM 1 のセッションに選択したアドレスが FWSM 2 のセッションに選択したアドレスと異なります。

接続タイムアウト

特定の接続に 2 分間トラフィックがない場合、接続はタイムアウトになります。Properties > Timeouts > Connection チェックボックスを使用して、このデフォルトを上書きできます。標準 TCP 接続は、デフォルトで 60 分後にタイムアウトになります。

Rule Actions > Connection Settings タブ

Connection Settings タブでは、最大接続数、最大初期接続、およびホストまたはネットワークでの TCP パケットのランダム化で使用するシーケンス番号を設定できます。また、接続タイムアウトと TCP 正規化も設定できます。

フィールド

- Maximum Connections：同時 TCP、UDP 接続、および初期接続の最大接続数を設定します。
  - Maximum TCP and UDP Connections : サブネット全体の同時 TCP および UDP 接続の最大接続数を 65,536 に指定します。両方のプロトコルのデフォルトは、0 で、これが最大接続数となります。
- Randomize Sequence Number : Randomize Sequence Number 機能の状態を、イネーブルまたはディセーブルに設定します。TCP の初期シーケンス番号のランダム化は、別のインライン ファイアウォールがシーケンス番号をランダム化していれば、ディセーブルにできます。これは、両方のファイアウォールがこのアクションを実行する必要がないためです。ただし、両方のファイアウォールの ISN のランダム化をイネーブルにしてもトラフィックへの影響はありません。

  各 TCP 接続には、2 つの Initial Sequence Number（ISN; 初期シーケンス番号）があります。1 つはクライアントが生成し、もう 1 つはサーバが生成します。セキュリティ アプライアンスは、発信方向へ通過する TCP SYN の ISN をランダム化します。同一セキュリティ レベルの 2 つのインターフェイスが接続されている場合、ISN は、両方向の SYN でランダム化します。

保護されたホストの ISN をランダム化すると、攻撃者が新しい接続の次の ISN を予測できなくなり、新しいセッションを乗っ取ることができなくなります。

- TCP Timeout：接続タイムアウト ルールを指定します。
  - Embryonic Connection Timeout：初期接続スロットが解放されるまでのアイドル時間を指定します。接続のタイムアウトをディセーブルにするには、0:0:0 と入力します。接続時間は 5 分以上にする必要があります。デフォルトは 30 分です。
  - Half Closed Connection Timeout：ハーフ クローズ接続スロットが解放されるまでのアイドル時間を指定します。接続のタイムアウトをディセーブルにするには、0:0:0 と入力します。接続時間は 5 分以上にする必要があります。デフォルトは 10 分です。
  - Connection Timeout：接続スロットが解放されるまでのアイドル時間を指定します。接続のタイムアウトをディセーブルにするには、0:0:0 と入力します。接続時間は 5 分以上にする必要があります。デフォルトは 1 時間です。
  - Send reset to TCP endpoints before timeout：TCP エンドポイントがタイムアウトの前にリセットされるように指定します。
- Idle Timeout：アイドル タイムアウト ルールを指定します。
  - Idle Timeout：接続がドロップするまでのアイドル時間を指定します。接続のタイムアウトをディセーブルにするには、0:00:00 と入力します。接続時間は 5 分以上にする必要があります。デフォルトは 1 時間です。
- Advanced Options：TCP ステート バイパス ルールを指定します。
  - TCP State Bypass：TCP ステート バイパスをイネーブルにします。詳細については、P.20-20 の「TCP ステート バイパスの概要」を参照してください。

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
•	•	•	•	—

Edit Class Map

Edit Class Map ダイアログボックスでは、クラスマップの説明を追加または編集できます。

フィールド

- Description：クラスマップ説明の名前を追加または変更します。

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
•	•	•	•	—

Edit Rule

Edit Rule ダイアログボックスでは、既存のルールを変更できます。

フィールド

- Select an action：新しいルールのアクション タイプを決めます。Select an action リストから、Permit または Deny のいずれかを選択します。
  - Permit：すべての一致したトラフィックを許可します。
  - Deny：すべての一致したトラフィックを拒否します。
- Apply to traffic：ルールを適用するトラフィック タイプを決めます。
  - Incoming to source interface：送信元インターフェイスへの着信トラフィックを選択します。
  - Outgoing from destination interface : 宛先インターフェイスからの発信トラフィックを選択します。
- Syslog status：syslog がイネーブルかどうかを示します。
- More Options：アクセスリストのロギングをイネーブルにして、ロギング オプションを設定します。More Options ボタンにより、ロギング オプションを設定できます。このボタンにより、次の操作を実行できます。
  - デフォルトのロギング動作を使用する。
  - ルールのロギングをイネーブルにする。
  - ルールのロギングをディセーブルにする。
  - 許可と拒否のログ レベルとロギング間隔を設定する。このオプションは、Enable Logging チェックボックスをオンにします。

    詳細については、「Log Options」を参照してください。また、グローバル ロギング オプションの設定については、「Advanced Access Rule Configuration」を参照してください。
- Time Range：このルールに定義されている時間範囲をリストから選択します。
- New：このルールの新しい時間範囲を作成します。「Add Time Range」を参照してください。
- Source and Destination Host/Network IP Address：IP アドレスによってネットワークを識別するには、このボタンを選択します。
  - Interface：ホストまたはネットワークが常駐するインターフェイス。
  - IP address：ホストまたはネットワークの IP アドレス。
  - Browse：Select Host/Network ペインのオプションをクリックして既存のホストまたはネットワークを選択し、Name、Interface、IP address、および Mask の各ボックスに、選択したホストまたはネットワークのプロパティ値を入力します。
  - Mask：ホストまたはネットワークのサブネット マスク。
- Name：ネットワークを名前で特定するには、このボタンをクリックします。ホスト / ネットワークへの名前付けについては、Hosts/Networks タブを参照してください。

  ホストまたはネットワークの名前。このオプションを選択し、再びルールを開いて編集すると、ボタン選択が IP Address に復帰し、名前付きホスト / ネットワーク IP アドレス情報がフィールドに表示されます。
- Group：Hosts/Networks　タブでグループ化したネットワークとホストのグループを特定するには、このボタンをクリックします。
  - Interface：グループ内のホストおよびネットワークに接続されたインターフェイス。
  - Group：グループ名。
- Protocol and Service: TCP and UDP ボタン：そのルールの TCP/UDP プロトコルを選択します。Source Port 領域と Destination Port 領域で、アクセスリストがパケットを照合するために使用するポートを指定できます。
  - Source Port Service：HTTP または FTP など、サービスのリストからポート番号、ポートの範囲、またはウェルノウン サービス名を指定するには、このオプションをクリックします。

- Source Port Service：演算子リストは、アクセスリストがポートを照合する方法を指定します。次のいずれかの演算子を選択します。
- =：ポート番号と等しい。
- not = ：ポート番号と等しくない。
- >：ポート番号より大きい。
- <：ポート番号より小さい。
- range：その範囲のポート番号の 1 つと等しい。
- Source Port Service：サービスのリストから、ポート番号、ポート範囲、または HTTP や FTP などのウェルノウン サービス名を指定します。Browse ボタンをクリックすると Service 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 TCP または UDP サービスを選択できます。
- Source Port Service Group：Service Group リストからサービス グループを指定するには、このオプションをクリックします。

- Protocol and Service ICMP：ICMP タイプ ボックスで、ルールの ICMP タイプを指定します。Browse ボタンをクリックすると Service 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 ICMP タイプを選択できます。
- Protocol and Service IP：IP プロトコル ボックスで、そのルールの IP プロトコルを指定します。Browse ボタンをクリックすると Protocols 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 IP プロトコルを選択できます。
- Manage Service Groups：サービス グループを管理します。サービス グループを使用して、アクセスリストと照合させる複数の連続していないポート番号を特定できます。たとえば、HTTP、FTP、およびポート番号 5、8、9 をフィルタリングする場合は、これらのすべてのポートを含むサービス グループを定義します。サービス グループを使用しない場合は、ポートごとに個別のルールを作成する必要があります。

  TCP、UDP、および TCP-UDP のサービス グループを作成できます。TCP-UDP プロトコルを使用するサービス グループには、TCP または UDP プロトコルを使用するサービス、ポート、および範囲が含まれます。詳細については、「Manage Service Groups」を参照してください。
- Description：（オプション）アクセス ルールの説明を入力します。

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
•	•	•	•	—

Edit Service Policy Rule > Traffic Classification タブ

Traffic Classification タブでは、セキュリティ ポリシー ルールを適用するトラフィックの照合に使用する基準を指定できます。

フィールド

- Description：トラフィック分類の説明を指定します。
- Default Inspection Traffic：デフォルトの検査トラフィック ポリシーで指定された基準を使用します。
- Source and destination IP address (uses ACL)：アクセス コントロール リストを使用し、送信元と宛先 IP アドレスに基づいてトラフィックを照合します。このフィールドは、インターフェイス サービス ポリシーを使用して特定のインターフェイスにルールを適用する場合にのみ選択できます。
- TCP or UDP destination port：TCP または UDP 宛先ポートに基づいてトラフィックを照合します。
- Any traffic：トラフィック タイプに関係なくすべてのトラフィックを照合します。

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
•	•	•	•	—

SUNRPC Server

SUNRPC Server ペインには、FWSM を通過できる SunRPC サービスとそれらのタイムアウトがサーバ単位で表示されます。

フィールド

- Interface：SunRPC サーバが常駐するインターフェイスを表示します。
- IP Address：SunRPC サーバの IP アドレスを表示します。
- Mask：SunRPC サーバの IP アドレスのサブネット マスクを表示します。
- Service ID：FWSM を通過することを許可する、SunRPC プログラム番号、またはサービス ID を表示します。
- Protocol：SunRPC 転送プロトコル（TCP または UDP）を表示します。
- Port：SunRPC プロトコルのポート範囲を表示します。
- Timeout：SunRPC サービス トラフィックへのアクセスが閉じられるまでのアイドル時間を表示します。

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
•	•	•	•	—

Add/Edit SUNRPC Service

Add/Edit SUNRPC Service ダイアログボックスでは、FWSM を通過することを許可する SunRPC サービス、およびそれらの固有タイムアウトをサーバ単位で指定できます。

フィールド

- Interface：SunRPC サーバが常駐するインターフェイスを表示します。
- Protocol：SunRPC 転送プロトコル（TCP または UDP）を指定します。
- IP Address：SunRPC サーバの IP アドレスを指定します。
- Port：SunRPC プロトコルのポート範囲を指定します。
- Mask：SunRPC サーバの IP アドレスのサブネット マスクを指定します。
- Timeout：SunRPC サービス トラフィックへのアクセスが閉じられるまでのアイドル時間を指定します。形式は、HH:MM:SS です。
- Service ID：FWSM を通過することを許可する、SunRPC プログラム番号、またはサービス ID 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
•	•	•	•	—