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 ルールでは、特定の種類のアプリケーション検査を、セキュリティ アプライアンス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。

サービス ポリシー ルールの設定

この項では、サービス ポリシー ルール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。

Service Policy Rules

Configuration > Security Policy > Service Policy Rules

一部のアプリケーションは、セキュリティ アプライアンス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、セキュリティ アプライアンス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。

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します。
- 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 ドロップダウン リスト：Interface、Source、Destination、Service、または Rule Query の中から、フィルタの基準を選択します。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することができます。

- Filter フィールド : 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。リストでは、インターフェイス名または **All Interfaces** を選択できます。Rule Query タイプの場合は、ドロップダウン リストに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 タイプとしては、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：ルールのイネーブル / ディセーブルを示します。
- 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を表示します。
- 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

Add Service Policy Rule Wizard > 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 領域
  - 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

Configuration > Security Policy > Service Policy Rules > 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

Add/Edit Service Policy Rule Wizard > 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 領域：
  - 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。
  - Tunnel Group：トンネル グループに基づいてトラフィックを照合します。
  - 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 : ドロップダウン 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

Add/Edit Service Policy Rule Wizard > Traffic Classification Criteria > 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。

Management Type Traffic Class and Action

Add/Edit Service Policy Rule Wizard > Management Type Traffic Class and Action

Management Class ダイアログボックスでは、管理トラフィック分類を設定し、分類されたトラフィックのアクションを定義できます。

フィールド

- Name：トラフィック管理クラスの名前を特定します。
- Description (optional)：新しいトラフィック管理クラスの説明をテキストで入力します。
- Match on Destination Port 領域：
  - Protocol：TCP または UDP の宛先ポートに基づいてトラフィックを照合します。
  - Service：=（等号）演算子または範囲を選択して、ポート範囲を指定します。番号を入力するか、またはドロップダウン リストからウェルノウン ポート名を選択します。範囲指定する場合は、両端の番号を指定する必要があります。
- Protocol Inspection 領域：
  - RADIUS Accounting Map：ドロップダウン リストから定義済みの RADIUS アカウンティング マップを選択します。
- Configure：Select RADIUS Accounting Map ダイアログボックスを開き、定義済み RADIUS アカウンティング マップを選択するか、RADIUS アカウンティング マップを追加することにより、検査機能をきめ細かく制御します。

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 RADIUS Accounting Map

Add/Edit Service Policy Rule Wizard > Management Type Traffic Class and Action > 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/Edit Service Policy Rule Wizard > Management Type Traffic Class and Action > Select RADIUS Accounting Map > 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 マップの説明を入力します（最大 100 文字）。
- 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
•	•	•	•	—

デフォルトの検査トラフィック基準の使用

PIX Firewall Version 6.3 およびそれ以前のリリースで使用できた **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、セキュリティ アプライアンス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、セキュリティ アプライアンスは、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 21-1 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 21-1　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
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
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、セキュリティ アプライアンス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。QoS Settings タブと 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** パネルで **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 パネルの **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 パネルの **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** パネルで **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**
- **QoS**

ステップ 7　**Finish** をクリックします。

Security Policy パネルの **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 パネルの **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）

- **Add/Edit Service Policy Rule Wizard > Traffic Match > Source and Destination Address**
- **Configuration > Security Policy > Edit Service Policy Rule > ACL タブ**

（このダイアログボックスに移動するパスは数種類あります。）

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 領域
  - 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 領域
  - 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、領域内に、Interface ドロップダウン リスト、IP address フィールド、. . . ボタン、および Mask ドロップダウン 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、領域内に Name ドロップダウン 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、領域内に Interface ドロップダウン リストと Group ドロップダウン 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。ドロップダウン 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。このフィールドは、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、事前に設定されたドロップダウン 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 フィールドに入力したアドレスのサブネット マスクを指定します。このフィールドは、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。このドロップダウン 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。ドロップダウン リストの項目は、Hosts/Networks ウィンドウで制御されます。このウィンドウの詳細については、「Network Object Groups」を参照してください。Group ドロップダウン 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 領域
  - 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、領域内に、Interface ドロップダウン リスト、IP address フィールド、. . . ボタン、および Mask ドロップダウン 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、領域内に Name ドロップダウン 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、領域内に Interface ドロップダウン リストと Group ドロップダウン 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。このドロップダウン 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。このフィールドは、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、事前に設定されたドロップダウン 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 フィールドに入力したアドレスのサブネット マスクを指定します。このフィールドは、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。このドロップダウン 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。ドロップダウン リストの項目は、Hosts/Networks ウィンドウで制御されます。このウィンドウの詳細については、「Network Object Groups」を参照してください。Group ドロップダウン 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：セキュリティ アプライアンス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 領域
  - 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。ドロップダウン 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。ドロップダウン リストから range を選択すると、2 つのフィールドが表示されます。それらのフィールドに、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。ドロップダウン 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。ドロップダウン 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。ドロップダウン リストから range を選択すると、2 つのフィールドが表示されます。それらのフィールドに、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。ドロップダウン 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、事前に設定されたドロップダウン 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、事前に設定されたドロップダウン 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

Add/Edit Service Policy Rule Wizard > Traffic Match > 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選択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。

  ドロップダウン 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。

  ドロップダウン リストから range を選択すると、2 つのフィールドが表示されます。それらのフィールドに、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
•	•	•	•	—

RTP Ports

Add/Edit Service Policy Rule Wizard > Traffic Match > RTP Ports

RTP Ports ダイアログボックスは、Traffic Match Criteria ダイアログボックスで RTP range 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選択する場合に表示されます。このダイアログボックスでは、RTP ポートの範囲に基づいて、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。

- RTP Port Range：トラフィックの照合で使用される RTP ポートの範囲を示す開始ポートと終了ポートを指定します。RTP ポート番号は、2000 ～ 65535 の範囲で指定します。範囲内の RTP ポートの最大数は 16383 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
•	•	•	•	—

IP Precedence

Add/Edit Service Policy Rule Wizard > Traffic Match > IP Precedence

IP Precedence ダイアログボックスは、Traffic Match Criteria ダイアログボックスで IP Precedence 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選択する場合に表示されます。このダイアログボックスでは、IP precedence 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

- Available IP Precedence：トラフィックの照合に使用できる使用可能な IP Precedence 値を一覧表示します。IP Precedence は、IP トラフィックに QoS プライオリティを割り当てる 1 つのモデルです。
- Add：選択した IP Precedence 値を Match on IP Precedence リストに追加します。
- Delete：選択した IP Precedence 値を Match on IP Precedence リストから削除します。
- Match On IP Precedence：トラフィックを照合するために選択された IP Precedence 値を一覧表示します。

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
•	•	•	•	—

IP DiffServ CodePoints (DSCP)

Add/Edit Service Policy Rule Wizard > Traffic Match > IP DiffServ CodePoints (DSCP)

IP DiffServ Code Points (DSCP) ダイアログボックスでは、QoS の Differentiated Services モデルに割り当てられた値に基づいて、トラフィックを照合できます。DiffServ では、EF と AF という 2 つの DSCP 値のセットを定義します。

フィールド

- Expedited Forwarding (EF)：マーク付きパケットにネットワークの最高レベルのサービスを付与する、1 つの DSCP 値（101110）を提供します。EF は一般に、Voice over IP（VoIP）の場合に最適です。
- Assured Forwarding (AF)：それぞれが 3 つのドロップ優先レベルを持つ 4 つのクラスを提供します。

選択ドロップダウン リストから名前付き DSCP 値を選択するか、または数値を入力できます。

- Named DSCP Values：照合基準として選択できる名前付き DSCP 値を一覧表示します。照合する値を選択し、**Add** を選択します。
- Enter DSCP value (0-63)：数字の DSCP 値を指定します。
- Add：選択した DSCP 値を Match on DSCP テーブルに追加します。
- Delete：選択した DSCP 値を Match on DSCP テーブルから削除します。
- Match on DSCP：照合基準として選択された DSCP 値を一覧表示します。
- Enter DSCP value (0-63)：照合用の基準として数値を使用します。

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
•	•	•	•	—

Rule Actions > Protocol Inspection タブ

Add/Edit Service Policy Rule Wizard > Rule Actions > Protocol Inspection タブ
（このタブに移動するパスは数種類あります。）

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.6-30 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：Select DCERPC 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。
- 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：Select DNS 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。
- 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。
  - Configure：Select ESMTP 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。
- 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 H323 H225 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。
  - Configure：Select H323 RAS 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。
- 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。
- IM：IM 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 IM 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。
- IPSec-Pass-Thru：IPSec 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 IPSec 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。
- 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。
  - Configure：Select NETBIOS 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。
- 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。
- SCCP 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。
  - Configure：Select SCCP (Skinny) 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。
- 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。
- 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。
- 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
•	•	•	•	—

参考資料

検査マップの設定

『*Cisco Security Appliance Command Reference*』にあるプロトコルごとの Inspect コマンド ページ

Select DCERPC Map

Add/Edit Service Policy Rule Wizard > Rule Actions > Protocol Inspection タブ > Select DCERPC Map

Select DCERPC Map ダイアログボックスでは、新しい DCERPC マップを選択または作成できます。DCERPC マップにより、DCERPC 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 DCERPC Map テーブルには、アプリケーション検査で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

- No DCERPC map for inspection：DCERPC マップを指定しません。
- Select a DCERPC map for fine control over inspection：定義済みのアプリケーション検査マップを選択するか、新しいマップを追加できます。
- Add：その検査の Add Policy Map ダイアログボックスを開きます。

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

Add/Edit Service Policy Rule Wizard > Rule Actions > Protocol Inspection タブ > Configure DNS

フィールド

Maximum DNS packet length (default 512)：セキュリティ アプライアンス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 DNS Map

Add/Edit Service Policy Rule Wizard > Rule Actions > Protocol Inspection タブ > Select DNS Map

Select DNS Map ダイアログボックスでは、新しい DNS マップを選択または作成できます。DNS マップにより、DNS 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 DNS Map テーブルには、アプリケーション検査で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

- No DNS map for inspection：DNS マップを指定しません。
- Select a DNS map for fine control over inspection：定義済みのアプリケーション検査マップを選択するか、新しいマップを追加できます。
- Add：その検査の Add Policy Map ダイアログボックスを開きます。

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 ESMTP Map

Add/Edit Service Policy Rule Wizard > Rule Actions > Protocol Inspection タブ > Select ESMTP Map

Select ESMTP Map ダイアログボックスでは、新しい ESMTP マップを選択または作成できます。ESMTP マップにより、ESMTP 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 ESMTP Map テーブルには、アプリケーション検査で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

- No ESMTP map for inspection：ESMTP マップを指定しません。
- Select an ESMTP map for fine control over inspection：定義済みのアプリケーション検査マップを選択するか、新しいマップを追加できます。
- Add：その検査の Add Policy Map ダイアログボックスを開きます。

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 FTP Map

Add/Edit Service Policy Rule Wizard > Rule Actions > Protocol Inspection タブ > 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、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で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。これによってセキュリティ アプライアンスは、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。
- No FTP map for inspection：FTP マップを指定しません。
- Select an FTP map for fine control over inspection : 定義済みのアプリケーション検査マップを選択するか、新しいマップを追加できます。
- Add：その検査の Add Policy Map ダイアログボックスを開きます。

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

Add/Edit Service Policy Rule Wizard > Rule Actions > Protocol Inspection タブ >　Select GTP Map

Select GTP Map ダイアログボックスでは、新しい GTP マップを選択または作成できます。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で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セキュリティ アプライアンスで GTP アプリケーション検査のイネーブル化を試みると、セキュリティ アプライアンスはエラー メッセージを表示します。

フィールド

- No GTP map for inspection：GTP マップを指定しません。
- Select an GTP map for fine control over inspection : 定義済みのアプリケーション検査マップを選択するか、新しいマップを追加できます。
- Add：その検査の Add Policy Map ダイアログボックスを開きます。

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.323 Map

Add/Edit Service Policy Rule Wizard > Rule Actions > Protocol Inspection タブ > Select H.323 Map

Select H.323 Map ダイアログボックスでは、新しい H.323 マップを選択または作成できます。H.323 マップにより、H.323 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.323Map テーブルには、アプリケーション検査で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

- No H.323 map for inspection：H.323 マップを指定しません。
- Select an H.323 map for fine control over inspection：定義済みのアプリケーション検査マップを選択するか、新しいマップを追加できます。
- Add：その検査の Add Policy Map ダイアログボックスを開きます。

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

Add/Edit Service Policy Rule Wizard > Rule Actions > Protocol Inspection タブ > Select HTTP Map

Select HTTP Map ダイアログボックスでは、新しい HTTP マップを選択または作成できます。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で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

- No HTTP map for inspection：HTTP マップを指定しません。
- Select an HTTP map for fine control over inspection：定義済みのアプリケーション検査マップを選択するか、新しいマップを追加できます。
- Add：その検査の Add Policy Map ダイアログボックスを開きます。

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 IM Map

Add/Edit Service Policy Rule Wizard > Rule Actions > Protocol Inspection タブ > Select IM Map

Select IM Map ダイアログボックスでは、新しい IM マップを選択または作成できます。IM マップにより、IM 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 IM Map テーブルには、アプリケーション検査で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

- No IM map for inspection：IM マップを指定しません。
- Select an IM map for fine control over inspection：定義済みのアプリケーション検査マップを選択するか、新しいマップを追加できます。
- Add：その検査の Add Policy Map ダイアログボックスを開きます。

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 IPSec-Pass-Thru Map

Add/Edit Service Policy Rule Wizard > Rule Actions > Protocol Inspection タブ > Select IPSec-Pass-Thru Map

Select IPSec-Pass-Thru ダイアログボックスでは、新しい IPSec マップを選択または作成できます。IPSec マップにより、IPSec 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 IPSec Map テーブルには、アプリケーション検査で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

- No IPSec map for inspection：IPSec マップを指定しません。
- Select an IPSec map for fine control over inspection：定義済みのアプリケーション検査マップを選択するか、新しいマップを追加できます。
- Add：その検査の Add Policy Map ダイアログボックスを開きます。

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

Add/Edit Service Policy Rule Wizard > Rule Actions > Protocol Inspection タブ > Select MGCP Map

Select MGCP Map ダイアログボックスでは、新しい MGCP マップを選択または作成できます。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で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

- No MGCP map for inspection：MGCP マップを指定しません。
- Select an MGCP map for fine control over inspection: 定義済みのアプリケーション検査マップを選択するか、新しいマップを追加できます。
- Add：その検査の Add Policy Map ダイアログボックスを開きます。

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 NETBIOS Map

Add/Edit Service Policy Rule Wizard > Rule Actions > Protocol Inspection タブ > Select NetBIOS Map

Select NETBIOS Map ダイアログボックスでは、新しい NetBIOS マップを選択または作成できます。NetBIOS マップにより、NetBIOS 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 NetBIOS Map テーブルには、アプリケーション検査で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

- No IM map for inspection：NetBIOS マップを指定しません。
- Select a NetBIOS map for fine control over inspection：定義済みのアプリケーション検査マップを選択するか、新しいマップを追加できます。
- Add：その検査の Add Policy Map ダイアログボックスを開きます。

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 SCCP (Skinny) Map

Add/Edit Service Policy Rule Wizard > Rule Actions > Protocol Inspection タブ > Select SCCP Map

Select SCCP (Skinny) Map ダイアログボックスでは、新しい SCCP (Skinny) マップを選択または作成できます。SCCP (Skinny) マップにより、SCCP (Skinny) 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 SCCP (Skinny) Map テーブルには、アプリケーション検査で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

- No SCCP (Skinny) map for inspection：SCCP (Skinny) マップを指定しません。
- Select an SCCP (Skinny) map for fine control over inspection：定義済みのアプリケーション検査マップを選択するか、新しいマップを追加できます。
- Add：その検査の Add Policy Map ダイアログボックスを開きます。

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

Add/Edit Service Policy Rule Wizard > Rule Actions > Protocol Inspection タブ > Select SIP Map

Select SIP Map ダイアログボックスでは、新しい SIP マップを選択または作成できます。SIP マップにより、SIP 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 SIP Map テーブルには、アプリケーション検査で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

- No SIP map for inspection：SIP マップを指定しません。
- Select a SIP map for fine control over inspection：定義済みのアプリケーション検査マップを選択するか、新しいマップを追加できます。
- Add：その検査の Add Policy Map ダイアログボックスを開きます。

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

Add/Edit Service Policy Rule Wizard > Rule Actions > Protocol Inspection タブ > Select SNMP Map

Select SNMP Map ダイアログボックスでは、新しい SNMP マップを選択または作成できます。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で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

- No SNMP map for inspection：SNMP マップを指定しません。
- Select an SNMP map for fine control over inspection : 定義済みのアプリケーション検査マップを選択するか、新しいマップを追加できます。
- Add：その検査の Add Policy Map ダイアログボックスを開きます。

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 > Intrusion Prevention タブ

Add/Edit Service Policy Rule Wizard > Rule Actions > Intrusion Prevention タブ

Intrusion Prevention タブでは、1 つのトラフィック クラスのポリシー マップ内で実行される侵入防御のアクションを設定できます。このウィンドウは、セキュリティ アプライアンスに Intrusion Prevention System（IPS; 侵入防護システム）ハードウェアがインストールされている場合にのみ表示されます。

フィールド

- Enable IPS for this traffic flow：このトラフィック フローでの侵入防御をイネーブルまたはディセーブルにします。このチェックボックスをオンにすると、このウィンドウの他のパラメータがアクティブになります。
- Mode：侵入防御の動作モードを設定します。
  - Inline Mode：インライン モードを選択します。このモードでは、パケットが IPS に転送されます。パケットは、IPS の働きによりドロップされる場合があります。
  - Promiscuous Mode：無差別モードを選択します。このモードでは、元のパケットの複製パケットに対して IPS が作動します。元のパケットがドロップされることはありません。

- If IPS card fails, then：IPS カードが動作不能になった場合に実行するアクションを設定します。
  - Permit traffic：IPS カードで障害が発生した場合はトラフィックを許可します。
  - Close traffic：IPS カードで障害が発生した場合はトラフィックをブロックします。

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
•	•	•	•	—

Rule Actions > CSC Scan タブ

Add/Edit Service Policy Rule Wizard > Rule Actions > CSC Scan タブ

CSC Scan タブでは、Content Security and Control（CSC）SSM により、現在のトラフィック クラスによって識別されるトラフィックをスキャンするかどうかを指定できます。このウィンドウは、セキュリティ アプライアンスに CSC SSM がインストールされている場合にのみ表示されます。

CSC SSM は、HTTP、SMTP、POP3、および FTP のトラフィックのみをスキャンします。使用するサービス ポリシーで、これら 4 種類のプロトコル以外のプロトコルを含むトラフィックを選択すると、他のプロトコルのパケットは、スキャンされることなく CSC SSM を通過します。

CSC SSM の負荷を軽減するには、CSC SSM にパケットを送信するサービス ポリシー ルールで、HTTP、SMTP、POP3、または FTP パケットのみを選択するように設定します。

フィールド

- Enable CSC scan for this traffic flow：このトラフィック フローでの CSC SSM の使用をイネーブルまたはディセーブルにします。このチェックボックスをオンにすると、このウィンドウの他のパラメータがアクティブになります。
- If CSC card fails, then：CSC SSM が動作不能になった場合に実行するアクションを設定します。
  - Permit traffic：CSC SSM で障害が発生した場合はトラフィックを許可します。
  - Close traffic：CSC SSM で障害が発生した場合はトラフィックをブロックします。

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
•	•	•	•	—

参考資料

CSC SSM の管理

Rule Actions > Connection Settings タブ

Add/Edit Service Policy Rule Wizard > Rule Actions > Connection Settings タブ
（このタブに移動するパスは数種類あります。）

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 領域
  - 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。
  - Per Client Connections：クライアントごとに、同時接続できる TCP 接続と UDP 接続の最大数を指定します。クライアントあたりの最大接続数の接続をすでに開いているクライアントが新しい接続を試みると、セキュリティ アプライアンスは、その接続を拒否してパケットをドロップします。
  - Per Client Embryonic Connections：クライアントごとに、同時接続できる TCP 初期接続の最大数を指定します。クライアントあたりの最大初期接続数の接続をセキュリティ アプライアンスからすでに開いているクライアントが新しい TCP 接続を要求すると、セキュリティ アプライアンスは、その要求の処理を TCP 代行受信機能に代行させ、接続を阻止します。
- 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。この機能は、別のインライン セキュリティ アプライアンスもシーケンス番号をランダム化していて、結果としてデータ順序が変わる場合にのみディセーブルにしてください。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、高位のセキュリティ インターフェイスで動作するホスト / サーバによって生成される ISN をランダム化します。少なくとも 1 つの ISN をランダムに生成して、攻撃者が次の ISN を予想してセッションを乗っ取ることができないようにする必要があります。
- TCP Timeout 領域
  - Connection Timeout：接続スロットを解放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、0:0:0 と入力します。継続時間は 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：セキュリティ アプライアンスが、接続スロットを解放する前に接続のエンドポイントに TCP リセット メッセージを送信するように指定します。
  - 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。デフォルトは 30 秒です。
  - 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。継続時間は 5 分以上にする必要があります。デフォルトは 10 分です。

- TCP Normalization 領域
  - Use TCP Map：TCP 正規化をイネーブルにするかどうかを選択します。TCP マップを使用するには、この機能をイネーブルにします。
  - TCP Map：既存の TCP マップを選択します。
  - New：新しい TCP マップを追加します。
  - Edit：既存の TCP マップを編集します。

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
•	•	•	•	—

Rule Actions > QoS タブ

Add/Edit Service Policy Rule Wizard > Rule Actions > QoS タブ
（このタブに移動するパスは数種類あります。）

QoS タブでは、厳密なスケジュール プライオリティとレート制限トラフィックを適用できます。

制限事項

既存の VPN クライアント トラフィック、LAN-to-LAN トラフィック、または非トンネル トラフィックが確立されているインターフェイスを対象として、サービス ポリシーを適用または削除した場合、QoS ポリシーは適用されず、トラフィック ストリームから削除されません。このような接続を対象として QoS ポリシーを適用または削除するには、接続を消去（ドロップ）して再確立する必要があります。

フィールド

- Enable Priority for this flow：このフローでの厳密なスケジュール プライオリティをイネーブルまたはディセーブルにします。プライオリティ（LLQ）は、プライオリティ キューが設定されていなければ有効になりません。プライオリティ キューを設定するには、**Configuration > Properties > Priority Queue** を選択します。詳細については、「Priority Queue」を参照してください。
- Enable policing：入力方向または出力方向でのトラフィックのポリシングをイネーブルにします。
  - Direction：ポリシングを入力方向または出力方向のどちらでイネーブルにするかを選択します。
  - Committed Rate：このトラフィック フローのレート制限。これは、8000 ～ 2000000000 の範囲の値で、許容最大速度（bps）を指定します。
  - Conform Action：レートが適合バースト値未満の場合に実行するアクション。値は、transmit または drop です。
  - Exceed Action：レートが適合レート値と適合バースト値の間になっている場合にこのアクションを実行します。値は、transmit または drop です。
  - Burst Rate：1000 ～ 512000000 の範囲の値で、適合レート値までトラフィックを抑制するまでに、持続したバーストにおいて許可される瞬間的なバイト数を指定します。

（注）　Enable Policing チェックボックスをオンにすると、最大速度とバースト レートが適用され、適合レート値になるよう強制されます。*適合アクション*または*超過アクション*の指定があっても、それらは適用されません。

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

Configuration > Features > Security Policy > Edit > 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

Configuration > Security Policy > Access Rules > 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 タイプを決定します。Select an action ドロップダウン 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のタイプを決定します。
  - 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：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、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：ドロップダウン リストからこのルールに定義されている時間範囲を選択します。
- 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** ウィンドウの下のオプションを選択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 の各フィールドに、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することができます。
  - 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、このボタンを選択します。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、このボタンを選択します。
  - 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 ボタンと UDP ボタン：ルールの TCP/UDP プロトコルを選択します。Source Port 領域と Destination Port 領域では、パケットの照合のためにアクセスリストで使用されるポートを指定できます。
  - Source Port Service：サービスのドロップダウン 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 サービス名を指定するには、このオプションを選択します。
  - Source Port Service：演算子のドロップダウン リストで、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：範囲内のいずれかのポート番号と等しい。
  - Source Port Service：サービスのドロップダウン 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、事前に設定されたドロップダウン 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 ドロップダウン リストからサービス グループを指定するには、このオプションを選択します。

- Protocol and Service: ICMP : ICMP タイプのフィールドで、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、事前に設定されたドロップダウン リストから ICMP タイプを選択できます。
- Protocol and Service: IP : IP プロトコルのフィールドで、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、事前に設定されたドロップダウン 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 プロトコルのサービス グループには、TCP または UDP プロトコルのどちらかを使用する可能性があるサービス、ポート、および範囲が含まれています。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

Configuration > Security Policy > 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ている基準を使用します。
- 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。
- Tunnel Group：トンネル グループに基づいてトラフィックを照合します。
- 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。

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
•	•	•	•	—

Tunnel Group

Add Service Policy Rule Wizard >Traffic Match > Tunnel Group

Tunnel Group ダイアログボックスにより、トンネル グループに基づいて、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

- Tunnel Group：トラフィックの照合を行うトンネル グループを選択します。
- New：Add Tunnel Group ウィンドウを表示します。このウィンドウでは、新しいトンネル グループを設定できます。
- Match flow destination IP address : トンネル グループとともに、フロー宛先の IP アドレスを照合する場合の要件を追加します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

SUNRPC Server

Configuration > Properties > SUNRPC Server

SUNRPC Server ウィンドウには、セキュリティ アプライアンスを通過できる 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：セキュリティ アプライアンス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

Configuration > Properties > SUNRPC Server > Add/Edit SUNRPC Service

Add/Edit SUNRPC Service ダイアログボックスでは、セキュリティ アプライアンス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ビス単位で指定できます。

フィールド

- Interface Name：SunRPC サーバが常駐するインターフェイスを指定します。
- 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：セキュリティ アプライアンス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
•	•	•	•	—