CHAPTER 10

ファイアウォール ポリシー

ファイアウォール ポリシー機能を使用すると、アクセス ルール、CBAC インスペクション ルールなどのファイアウォール設定を、それらのルールによってトラフィックをフィルタするインターフェイスのコンテキストで表示したり変更したりできます。ルータとそのインターフェイスの図を使用して、ルータの別のインターフェイスを選択したり、そのインターフェイスにアクセス ルールまたはインスペクション ルールが適用されているかどうかを確認したりできます。また、［ファイアウォール ポリシー /ACL の編集］ウィンドウ内のルールの詳細を表示することもできます。

ファイアウォール ポリシー /ACL の編集

［ファイアウォール ポリシー /ACL の編集］ウィンドウでは、アクセス ルールとインスペクション ルールが関連付けられているインターフェイスを表示するコンテキストでそれらのルールを表示できます。表示されたアクセス ルールやインスペクション ルールを変更することもできます。

ファイアウォール ポリシー機能の使用前にファイアウォールを設定する

［ファイアウォール ポリシー /ACL の編集］ウィンドウを使用する前に、次の操作を実行する必要があります。

1. **LAN インターフェイスと WAN インターフェイスを設定します。**ファイアウォールを作成する前に、LAN インターフェイスと WAN インターフェイスを設定する必要があります。LAN ウィザードと WAN ウィザードを使用してルータの接続を設定できます。
2. **ファイアウォール ウィザードを使用してファイアウォールと DMZ を設定します。**ファイアウォール ウィザードは、指定した内部インターフェイスと外部インターフェイスにアクセス ルールやインスペクション ルールを適用するための最も簡単な方法です。このウィザードを使用して、DMZ インターフェイスを設定したり、DMZ ネットワークへのアクセスを許可するサービスを指定したりできます。
3. **作成したファイアウォール ポリシーを［ファイアウォール ポリシー］ウィンドウで編集します。**LAN インターフェイスと WAN インターフェイスを設定してファイアウォールを作成した後、このウィンドウを開いてトラフィック フローのポリシーを図で確認できます。アクセス ルールとインスペクション ルールのエントリを表示して、必要な変更を行うこともできます。

ファイアウォール ポリシー ビュー機能を使用する

ファイアウォールの作成後、［ファイアウォール ポリシー ビュー］ウィンドウを使用して、ルータ インターフェイスのコンテキストでファイアウォールの図を表示したり、必要に応じてファイアウォールを変更したりできます。

詳細については、実行する次のいずれかのアクションをクリックしてください。

- トラフィック フローを選択する
- トラフィック図を確認してトラフィック方向を選択する

- アクセス ルールを変更する
- インスペクション ルールを変更する

（注）　ファイアウォール フィーチャ セットをサポートしていない Cisco IOS イメージがルータで使用されている場合は、［サービス］エリアだけが表示され、アクセス コントロール エントリを作成することしかできません。

変更の適用ボタン

このウィンドウで行った変更をルータに配信する場合にクリックします。［変更の適用］ボタンをクリックせずに［ファイアウォール ポリシー /ACL の編集］ウィンドウを閉じようとすると、変更を適用するか、または破棄する必要があることを通知するメッセージが表示されます。

変更の破棄ボタン

このウィンドウで行った変更を破棄する場合にクリックします。このボタンをクリックしても、［変更の適用］ボタンを使用してルータに配信した変更は削除されません。

トラフィック フローを選択する

*トラフィック フロー*は、指定したインターフェイス（*送信元*インターフェイス）でルータに入り、指定したインターフェイス（*宛先*インターフェイス）でルータから出るトラフィックを示します。Cisco Router and Security Device Manager（Cisco CP）のトラフィックフロー表示コントロールは、［ファイアウォール ポリシー /ACL の編集］ウィンドウの上部に配置されています。

（注）　ルータには少なくとも 2 つのインターフェイスが設定されている必要があります。1 つしか設定されていない場合は、インターフェイスをもう 1 つ設定するように指示するメッセージが表示されます。

次の表は、Cisco CP のトラフィックフロー表示コントロールの定義を示しています。

送信元	目的のトラフィック フローが入るときに経由するインターフェイスを選択します。ファイアウォールは送信元インターフェイスに接続されたネットワークを保護します。［送信元］ドロップダウン リストには、設定済み IP アドレスを持つインターフェイスだけが表示されます。
宛先	トラフィックがルータから出るときに経由するインターフェイスを選択します。［宛先］ドロップダウン リストには、設定済み IP アドレスを持つインターフェイスだけが表示されます。
	［詳細］ボタン。インターフェイスの詳細を表示する場合にクリックします。IP アドレス、カプセル化タイプ、関連付けられている IPSec ポリシー、認証タイプなどの詳細情報が表示されます。
実行ボタン	選択したインターフェイスの情報でトラフィック フローの図を更新する場合にクリックします。図は、このボタンをクリックするまでは更新されません。送信元インターフェイスか宛先インターフェイスを選択していない場合、または送信元と宛先のインターフェイスが同じ場合、［実行］ボタンは無効になります。
表示オプション	［送信元］および［宛先］ドロップダウン リストから選択したインターフェイスを入れ替えるには、［発信元 / 宛先インターフェイスの入れ替え］を選択します。送信元インターフェイスに接続されたネットワークと宛先インターフェイスに接続されたネットワークの両方を保護するファイアウォールを作成する場合にこのオプションを使用できます。あるアクセス ルールが送信元インターフェイスに適用され、別のアクセス ルールが宛先インターフェイスの選択したトラフィック方向に適用されている場合は、［トラフィック フローのすべての ACL を表示する］を選択できます。両方のアクセス ルールのエントリが別のウィンドウに表示されます。

［送信元］および［宛先］ドロップダウン リストには、IP アドレスを持つインターフェイスがアルファベット順に表示されます。デフォルトでは、［送信元］リストの最初のインターフェイスと［宛先］リストの 2 番目のインターフェイスが選択されます。［送信元］および［宛先］ドロップダウン リストを使用して、別のトラフィック フローを選択します。選択したトラフィック フローは、トラフィック フロー表示コントロールの下のトラフィック図に表示されます。

たとえば、ルータのインターフェイス Ethernet 0 に接続してルータのインターフェイス Serial 0 から出るネットワークのトラフィック フローを表示するには、次の手順に従います。

ステップ 1　［送信元］ドロップダウン リストから Ethernet 0 を選択します。

ステップ 2　［宛先］ドロップダウン リストから Serial 0 を選択します。

ステップ 3　［実行］をクリックします。

ステップ 4　［送信元］および［宛先］ドロップダウン リストのインターフェイスを入れ替えるには、［表示オプション］ドロップダウン リストから［発信元 / 宛先インターフェイスの入れ替え］を選択します。

アウトバウンド トラフィックとリターン トラフィックに適用されるアクセス ルールは異なる場合があります。トラフィック図でアウトバウンド トラフィックおよびリターン トラフィックの表示を入れ替える方法については、「トラフィック図を確認してトラフィック方向を選択する」を参照してください。

ステップ 5　［送信元］および［宛先］ドロップダウン リストの横にある［詳細］ボタンをクリックして、インターフェイスの IP アドレス、IPSec ポリシーなどの情報を示すウィンドウを表示します。

トラフィック図を使用して作業するには、「トラフィック図を確認してトラフィック方向を選択する」を参照してください。メインの［ファイアウォール ポリシー］ウィンドウの説明に戻るには、「ファイアウォール ポリシー /ACL の編集」を参照してください。

トラフィック図を確認してトラフィック方向を選択する

トラフィック図には、選択した送信元インターフェイスと宛先インターフェイスが設定されているルータが表示されます（詳細については、「トラフィック フローを選択する」を参照してください）。また、選択したトラフィック フローに適用されているルールのタイプと、ルールが適用されている方向も表示されます。

アウトバウンド トラフィック

送信元インターフェイスでルータに入り、宛先インターフェイスでルータから出るトラフィック フローを強調表示する場合にクリックします。この部分を強調表示すると、この方向のトラフィック フローに適用されているルールの詳細を確認できます。

リターン トラフィック

宛先インターフェイスでルータに入り、送信元インターフェイスでルータから出るトラフィック フローを強調表示する場合にクリックします。この部分を強調表示すると、リターン トラフィックに適用されているルールの詳細を確認できます。

アイコン

トラフィック フローでは、次のアイコンでルールが表されます。

	フィルタ記号は、アクセス ルールが適用されていることを示します。
	虫眼鏡は、インスペクション ルールが適用されていることを示します。

	ルータ内のファイアウォール アイコンは、アウトバウンド トラフィック フローにファイアウォールが適用されていることを示します。このアイコンは、次の条件が満たされている場合に表示されます。 • 送信元インターフェイスのインバウンド方向のアウトバウンド トラフィックにインスペクション ルールが適用され、宛先インターフェイスのインバウンド方向にアクセス ルールが適用されている。 • 宛先インターフェイスのインバウンド方向に適用されているアクセス ルールが拡張アクセス ルールであり、1 つ以上のエントリを含んでいる。 リターン トラフィックにファイアウォールが適用されている場合、ファイアウォール アイコンは表示されません。ファイアウォール機能は利用できるがトラフィック フローにファイアウォールが適用されていない場合は、トラフィック図の下に「IOS ファイアウォール：非アクティブ」と表示されます。
	アウトバウンド トラフィックに適用されるルールは右矢印で示されます。送信元インターフェイスのトラフィック ライン上のアイコンは、ルータへのインバウンド トラフィックをフィルタするルールが存在することを示します。宛先インターフェイスのトラフィック ライン上のアイコンは、ルータからのアウトバウンド トラフィックをフィルタするルールが存在することを示します。このアイコンの上にマウスを置くと、適用されているルールの名前が表示されます。
	リターン トラフィックに適用されるルールは左矢印で示されます。宛先インターフェイスのトラフィック ライン上のアイコンは、ルータへのインバウンド トラフィックをフィルタするルールが存在することを示します。送信元インターフェイスのトラフィック ライン上のアイコンは、ルータからのアウトバウンド トラフィックをフィルタするルールが存在することを示します。このアイコンの上にマウス カーソルを置くと、適用されているルールの名前が表示されます。

（注）　アイコンは図の特定のインターフェイス上に表示されますが、図で表現されていないトラフィックに適用されるアクセス コントロール エントリがファイアウォール ポリシーに含まれている場合があります。たとえば、［宛先］カラムにワイルドカード アイコンが含まれているエントリは（「アクセス ルールを変更する」を参照）、現在選択されている宛先インターフェイス以外のインターフェイスから出るトラフィックに適用される場合があります。ワイルドカード アイコンはアスタリスクとして表示され、ネットワークまたはホストを表します。

アクセス ルールに変更を加えるには、「アクセス ルールを変更する」を参照してください。メインの［ファイアウォール ポリシー］ウィンドウの説明に戻るには、「ファイアウォール ポリシー /ACL の編集」を参照してください。

アクセス ルールを変更する

ポリシー パネルには、選択したトラフィック フローに適用されているルールの詳細が表示されます。ポリシー パネルは、送信元インターフェイスと宛先インターフェイスを選択したとき、およびトラフィック図でアウトバウンド トラフィックとリターン トラフィックの強調表示を切り替えたときに更新されます。

エントリのないアクセス ルールがインターフェイスに関連付けられている場合、ポリシー パネルには何も表示されません。たとえば、CLI を使用してインターフェイスにルール名を関連付けたが、そのルールのエントリが作成されていない場合などです。ポリシー パネルに何も表示されない場合は、［追加］ボタンを使用してルールのエントリを作成できます。

サービス エリアのヘッダー フィールド

ファイアウォール機能	ルータで使用されている Cisco IOS イメージがファイアウォール機能をサポートしている場合は、このフィールドに［使用可能］と表示されます。
アクセス ルール	エントリが表示されているアクセス ルールの名前または番号が表示されます。
インスペクション ルール	エントリが表示されているインスペクション ルールの名前が表示されます。
	このアイコンは、アクセス ルールがインターフェイスに関連付けられているが、その名前または番号のアクセス ルールが作成されていない場合に表示されます。Cisco CP により、少なくとも 1 つのアクセス ルール エントリがなければポリシーは効果がないことを通知されます。

サービス エリアのコントロール

次の表に、［サービス］エリアのコントロールを示します。

追加ボタン	アクセス ルール エントリを追加する場合にクリックします。現在選択されているエントリの前と後のどちらに新しいエントリを追加するかを指定します。次に、［エントリの追加］ウィンドウでエントリを作成します。エントリの順番は重要です。［ファイアウォール ポリシー /ACL の編集］ウィンドウからエントリを追加すると、［拡張］エントリのダイアログが表示されます。標準ルール エントリを追加するには、［追加タスク］>［ACL エディタ］>［アクセス ルール］の順に選択します。
編集ボタン	選択したアクセス ルール エントリを編集する場合にクリックします。［ファイアウォール ポリシー /ACL の編集］ウィンドウでは拡張ルール エントリしか追加できませんが、選択したインターフェイスにすでに適用されている標準ルール エントリを編集することはできます。

切り取りボタン	選択したアクセス ルール エントリを削除する場合にクリックします。エントリはクリップボードに保存され、リスト内の別の位置に貼り付けたり、別のアクセス ルールに貼り付けたりできます。エントリを並べ替える場合は、ある場所からエントリを切り取り、そのエントリを配置する場所の前または後ろにあるエントリを選択して［貼り付け］をクリックします。［貼り付け］コンテキスト メニューを使用すると、選択したエントリの前または後ろにエントリを配置できます。
コピー ボタン	ルール エントリを選択してこのボタンをクリックすると、クリップボードにそのエントリがコピーされます。
貼り付けボタン	クリップボード上のエントリを選択したルールに貼り付ける場合にクリックします。現在選択されているエントリの前と後のどちらにエントリを貼り付けるかを確認するメッセージが表示されます。アクセス ルール内にすでに同じエントリが存在する場合は、表示される［拡張ルール エントリの追加］ウィンドウでそのエントリを変更できます。同じアクセス ルールに重複するエントリを配置することはできません。
インターフェイス ドロップダウン リスト	選択したトラフィック フロー（アウトバウンドまたはリターン トラフィック）に、送信元インターフェイスと宛先インターフェイスの両方に対するアクセス ルールが適用されている場合は、このリストを使用して 2 つのルールを切り替えることができます。

Apply Firewall	選択したトラフィック フローにファイアウォールが適用されていない場合は、［アウトバウンド トラフィック］を選択して［ファイアウォールの適用］ボタンをクリックすることによってファイアウォールを適用できます。デフォルトでは、［ファイアウォールの適用］をクリックすると、送信元インターフェイスのインバウンド方向に Cisco CP のデフォルトのインスペクション ルールが関連付けられ、宛先インターフェイスのインバウンド方向にトラフィックを拒否するアクセス ルールが関連付けられます。ルータで使用されている Cisco IOS イメージがファイアウォール機能をサポートしていない場合、このボタンは無効になります。たとえば、Ethernet 0 インターフェイスに接続されたネットワークを Ethernet 1 インターフェイスへのインバウンド トラフィックから保護するファイアウォールを適用するには、［送信元］ドロップダウン リストで Ethernet 0 を選択し、［宛先］ドロップダウン リストで Ethernet 1 を選択します。次に、［ファイアウォールの適用］をクリックします。Ethernet 1 インターフェイスに接続されたネットワークを Ethernet 0 インターフェイスへのインバウンド トラフィックから保護するファイアウォールを適用するには、［追加タスク］>［ACL エディタ］>［アクセス ルール］を選択します。

［サービス］エリアのボタンは、ルールが読み取り専用の場合は無効になります。ルールが読み取り専用になるのは、Cisco CP でサポートされていない構文がルールに含まれている場合です。読み取り専用のルールは、アイコン で示されます。

ファイアウォールが適用されるリターン トラフィック フローをフィルタする標準ルールが存在する場合は、その標準アクセス ルールを拡張ルールに変換することを通知するメッセージが表示されます。

サービス エリアのエントリ フィールド

次の表に、［サービス］エリアのエントリ内のアイコンとその他のデータを示します。

フィールド	説明	アイコン	意味
アクション	トラフィックが許可されるか拒否されるかを示す。		送信元トラフィックを許可する。
			送信元トラフィックを拒否する。
送信元 / 宛先	ネットワークまたはホストのアドレス、または任意のホストまたはネットワーク。		ネットワークのアドレス。
			ホストのアドレス。
			任意のネットワークまたはホスト。
サービス	フィルタが適用されるサービスのタイプ。		例 : TCP、EIGRP、UDP、GRE。「IP サービス」を参照してください。
			例 : Telnet、http、FTP。「TCP サービス」を参照してください。
			例 : SNMP、bootpc、RIP。「UDP サービス」を参照してください。
			インターネット グループ管理プロトコル（IGMP）。
			例 : echo-reply、host-unreachable。「ICMP メッセージ タイプ」を参照してください。
ログ	拒否したトラフィックをログに記録するかどうかを指定する。		拒否したトラフィックをログに記録する。ファイアウォールのロギングを設定するには、「ファイアウォール ログ」を参照してください。
オプション	CLI を使用して設定されるオプション。	アイコンなし。	
説明	提供されている説明。	アイコンなし。	

インスペクション ルールを変更する場合は、「インスペクション ルールを変更する」を参照してください。メインの［ファイアウォール ポリシー］ウィンドウの説明に戻るには、「ファイアウォール ポリシー /ACL の編集」を参照してください。

インスペクション ルールを変更する

［アプリケーション］エリアは、ルータで実行されている Cisco IOS イメージが CBAC インスペクション ルールをサポートしている場合に表示されます。［アプリケーション］エリアには、トラフィック フローをフィルタするインスペクション ルール エントリが表示され、新しいトラフィック フローが選択されるたびに更新されます。選択したトラフィックの方向に適用されているインスペクション ルールが表示されます。

［アプリケーション］エリアには、**アウトバウンド トラフィック**に対する次のいずれかのルールが表示されます。

- 送信元インターフェイスのインバウンド方向に適用されているインスペクション ルール（存在する場合）
- 送信元インターフェイスのインバウンド方向にインスペクション　ルールが適用されていない場合は、宛先インターフェイスのアウトバウンド方向に適用されているインスペクション ルール

送信元 / 宛先インターフェイスを入れ替えて他のルールを表示する

リターン トラフィックに適用されているインスペクション ルールは表示されません。表示するには、［表示オプション］メニューの［発信元 / 宛先インターフェイスの入れ替え］を選択します。［ファイアウォール ポリシー/ACL の編集］ウィンドウに表示されないインスペクション ルールも、［ファイアウォールと ACL］タスクの［アプリケーション セキュリティ］ウィンドウで確認できます。

⚠	このアイコンは、選択したトラフィック方向に 2 つのインスペクション ルールが検出された場合に表示されます。どちらか一方のインスペクション ルールの関連付けを解除するように警告するダイアログも表示されます。

アプリケーション エリアのコントロール

［アプリケーション］エリアには、次のコントロールが表示されます。

［追加］— インスペクション ルールを追加する場合にクリックします。インスペクション ルールがない場合は、Cisco CP のデフォルトのインスペクション ルールを追加するか、カスタム インスペクション ルールを作成して追加できます。

インスペクション ルールが適用されていないトラフィック フローに Cisco CP のデフォルトのインスペクション ルールを追加すると、そのルールは送信元インターフェイスへのインバウンド トラフィックに関連付けられます。インスペクション ルールが存在するかどうかにかかわらず、特定のアプリケーションのエントリを追加できます。

［編集］— 選択したエントリを編集する場合にクリックします。

［削除］— 選択したエントリを削除する場合にクリックします。

［グローバル設定］— グローバル タイムアウト値としきい値を設定できるダイアログ ボックスを表示する場合にクリックします。

［要約］— 各エントリのアプリケーションまたはプロトコル名と説明を表示する場合にクリックします。

［詳細］— 各エントリのアプリケーションまたはプロトコル名、説明、アラート ステータス、監査追跡ステータス、およびタイムアウト設定を表示する場合にクリックします。

アプリケーション エリアのエントリ フィールド

［アプリケーション］エリアには、次のエントリ フィールドがあります。

［アプリケーション プロトコル］— アプリケーションまたはプロトコルの名前を表示します。例：**vdolive**。

［アラート］— アラートがオン（デフォルト）かオフかを示します。

［監査追跡］— 監査追跡がオンかオフ（デフォルト）かを示します。

［タイムアウト］— ルータがこのプロトコルまたはアプリケーションのリターン トラフィックをブロックするまで待機する時間を秒単位で表示します。

［説明］— 簡単な説明を表示します。例：**VDOLive プロトコル**。

メインの［ファイアウォール ポリシー］ウィンドウの説明に戻るには、「ファイアウォール ポリシー /ACL の編集」を参照してください。

アプリケーション エントリの追加

このウィンドウでは、Cisco IOS ファイアウォールで検査するアプリケーション エントリを追加します。

アラート アクション

次のいずれかを選択します。

- ［デフォルト（オン）］— デフォルトのままにします。デフォルト値は［オン］です。
- ［オン］— アラートを有効にします。
- ［オフ］— アラートを無効にします。

監査アクション

次のいずれかを選択します。

- ［デフォルト（オフ）］— デフォルトのままにします。デフォルト値は［オフ］です。
- ［オン］— 監査証跡を有効にします。
- ［オフ］— 監査証跡を無効にします。

タイムアウト

ルータがこのプロトコルまたはアプリケーションのリターン トラフィックをブロックするまで待機する時間を指定します。フィールドには、プロトコルまたはアプリケーションのデフォルト値があらかじめ入力されています。

RPC アプリケーション エントリの追加

このウィンドウでは、RPC（リモート プロシージャ コール）プログラムの番号を追加して、アラート、監査、タイムアウト、および待機時間の設定を行います。

アラート アクション

次のいずれかを選択します。

- ［デフォルト（オン）］— デフォルトのままにします。デフォルト値は［オン］です。
- ［オン］— アラートを有効にします。
- ［オフ］— アラートを無効にします。

監査アクション

次のいずれかを選択します。

- ［デフォルト（オフ）］— デフォルトのままにします。デフォルト値は［オフ］です。
- ［オン］— 監査証跡を有効にします。
- ［オフ］— 監査証跡を無効にします。

タイムアウト

ルータがこのプロトコルまたはアプリケーションのリターン トラフィックをブロックするまで待機する時間を指定します。フィールドには、デフォルト値があらかじめ入力されています。

プログラム番号

このフィールドには、1 つのプログラム番号を入力します。

待機時間

必要に応じて、同じ送信元から同じ宛先アドレスとポートへの次の RPC 接続が確立されるまで待機する分数を指定できます。デフォルトの待機時間はゼロ（0）分です。

フラグメント アプリケーション エントリの追加

このウィンドウでは、［ファイアウォール ポリシー /ACL の編集］ウィンドウで設定しているインスペクション ルールにフラグメント エントリを追加したり、アラート、監査、およびタイムアウトの設定を指定したりできます。フラグメント エントリでは、ルータが受信する再設定されていないパケットの最大数を設定できます。この数を超えると、ルータはパケットの廃棄を開始します。

アラート アクション

次のいずれかを選択します。

- ［デフォルト（オン）］— デフォルトのままにします。デフォルト値は［オン］です。
- ［オン］— アラートを有効にします。
- ［オフ］— アラートを無効にします。

監査アクション

次のいずれかを選択します。

- ［デフォルト（オフ）］— デフォルトのままにします。デフォルト値は［オフ］です。
- ［オン］— 監査証跡を有効にします。
- ［オフ］— 監査証跡を無効にします。

タイムアウト

ルータがこのプロトコルまたはアプリケーションのリターン トラフィックをブロックするまで待機する時間を指定します。フィールドには、デフォルト値があらかじめ入力されています。

範囲（オプション）

ルータが受信する再設定されていないパケットの最大数を入力します。この数を超えると、ルータはパケットの廃棄を開始します。50 ～ 10,000 の範囲内の値を入力できます。

http アプリケーション エントリの追加 / 編集

このウィンドウでは、インスペクション ルールに http アプリケーションを追加します。

アラート アクション

次のいずれかを選択します。

- ［デフォルト（オン）］— デフォルトのままにします。デフォルト値は［オン］です。
- ［オン］— アラートを有効にします。
- ［オフ］— アラートを無効にします。

監査アクション

次のいずれかを選択します。

- ［デフォルト（オフ）］— デフォルトのままにします。デフォルト値は［オフ］です。
- ［オン］— 監査証跡を有効にします。
- ［オフ］— 監査証跡を無効にします。

タイムアウト

ルータがこのプロトコルまたはアプリケーションのリターン トラフィックをブロックするまで待機する時間を指定します。フィールドには、デフォルト値があらかじめ入力されています。

Java アプレットの送信元ホスト / ネットワーク

検査するアプレット トラフィックの送信元ホストまたはネットワークを指定します。複数のホストおよびネットワークを指定できます。

［Java アプレット ブロッキング］ウィンドウを表示してホストまたはネットワークを指定する場合は、［追加］をクリックします。

リストからエントリを削除する場合は、［削除］をクリックします。

Java アプレット ブロッキング

このウィンドウでは、指定したネットワークまたはホストからの Java アプレットを許可するか、または拒否するかを指定します。

アクション

次のいずれかを選択します。

- ［ブロックしない（許可）］— このネットワークまたはホストからの Java アプレットを許可します。
- ［ブロックする（拒否）］— このネットワークまたはホストからの Java アプレットを拒否します。

ホスト / ネットワーク

ネットワークまたはホストを指定します。

タイプ

次のいずれかを選択します。

- ［ネットワーク］— このタイプを選択する場合は、［IP アドレス］フィールドにネットワーク アドレスを入力します。ワイルドカード マスクを使用すると、1 つのネットワーク番号を入力するだけで複数のサブネットを指定できます。
- ［ホスト名または IP アドレス］— このタイプを選択する場合は、次のフィールドにホスト IP アドレスまたはホスト名を入力します。
- ［任意の IP アドレス］— このタイプを選択する場合は、指定したアクションが任意のホストまたはネットワークに適用されます。

IP アドレス / ワイルドカード マスク

ネットワーク アドレス、ワイルドカード マスクの順に入力して、ネットワーク アドレスのどの部分が正確に一致しなければならないかを指定します。

たとえば、ネットワーク アドレスとして 10.25.29.0 を、ワイルドカード マスクとして 0.0.0.255 を入力した場合、送信元アドレスに 10.25.29 を含む Java アプレットにフィルタがかけられます。ワイルドカード マスクとして 0.0.255.255 を入力した場合は、送信元アドレスに 10.25 を含む Java アプレットにフィルタがかけられます。

ホスト名 /IP

このフィールドは、タイプとして［ホスト名または IP アドレス］を選択した場合に表示されます。ホスト名を入力する場合は、ホスト名を IP アドレスに解決できる DNS サーバがネットワーク上に存在することを確認してください。

Cisco CP 警告：インスペクション ルール

このウィンドウは、トラフィック フローの方向に 2 つのインスペクション ルールが設定されている場合に表示されます。たとえば、あるインスペクション ルールが送信元インターフェイスへのインバウンド トラフィックに適用され、別のインスペクション ルールが宛先インターフェイスのアウトバウンド トラフィックに適用されている場合などです。2 つのインスペクション ルールを適用してもルータの動作に問題が生じるとは限りませんが、2 つのルールは不要です。Cisco CP では、インスペクション ルールをそのまま保持するか、送信元インターフェイスまたは宛先インターフェイスのどちらかのインスペクション ルールを削除することができます。

- ［変更しない］— どちらのインスペクション ルールも削除しません。
- ［< インターフェイス名 >　のインバウンド方向に対するインスペクション ルール < 名前 > の適用を保持し、< インターフェイス名 > のアウトバウンド方向に対するインスペクション ルール < 名前 > の適用を解除する］— 一方のインスペクション ルールを保持し、もう一方のインターフェイスとルールの関連付けを解除します。
- ［< インターフェイス名 > のアウトバウンド方向に対するインスペクション ルール < 名前 > の適用を保持し、< インターフェイス名 > のインバウンド方向に対するインスペクション ルール < 名前 > の適用を解除する］— 一方のインスペクション ルールを保持し、もう一方のインターフェイスとルールの関連付けを解除します。

オプションを選択して［OK］をクリックする前に、［キャンセル］をクリックして、保持するインスペクション ルールにエントリを追加する必要があるかどうかを判断できます。エントリを追加する場合は、［ファイアウォール ポリシー /ACL の編集］ウィンドウの［アプリケーション］エリアのツールバーにある［追加］ボタンを使用します。

Cisco CP 警告：ファイアウォール

このウィンドウは、［ファイアウォール ポリシー /ACL の編集］ウィンドウで［ファイアウォールの適用］をクリックすると表示されます。ルールが適用されるインターフェイスのリストとルールの説明が表示されます。

例：

```
SDM will apply firewall configuration to the following interfaces:
Inside (Trusted) Interface: FastEthernet 0/0
* Apply inbound default SDM Inspection rule
* Apply inbound ACL. Anti-spoofing, broadcast, local loopback, etc.).

Outside (Untrusted) Interface: Serial 1/0
* Apply inbound access list to deny returning traffic.
```

これらの変更を適用する場合は［OK］をクリックし、ファイアウォールの適用を中止する場合は［キャンセル］をクリックします。

ファイアウォール ポリシーの編集

［ファイアウォール ポリシーの編集］ウィンドウには、ルータに設定されているファイアウォール ポリシーの図が表示されます。また、このウィンドウを閉じずにポリシーに ACL を追加できます。このウィンドウで情報を表示したりルールを追加したりする方法については、以下のセクションの手順を参照してください。

このヘルプ トピックの内容は、次のとおりです。

このウィンドウに情報を表示する前に必要な作業

このウィンドウは、ゾーン、ゾーンペア、またはポリシー マップが設定されていない場合、空白になります。［設定］>［ファイアウォールと ACL］>［ファイアウォールの作成］を選択して拡張ファイアウォール ウィザードを実行し、これらの要素を含む基本設定を作成します。この作業が完了したら、必要に応じて追加のゾーン、ゾーン ペア、およびポリシーを作成できます。ゾーンを設定するには、［設定］>［追加タスク］>［ゾーン］の順に選択します。追加のゾーン ペアを設定するには、［追加タスク］>［ゾーン ペア］の順に選択します。

ゾーン ペアで使用するポリシー マップを作成するには、［設定］>［追加タスク］>［C3PL］を選択します。［ポリシー マップ］ブランチをクリックすると、追加のブランチが表示され、ポリシー マップ、およびポリシー マップのトラフィックを定義するクラス マップを作成できます。

ポリシーの表示の展開と縮小

ポリシーの表示が縮小されているときは、ポリシー名、送信元ゾーン、および宛先ゾーンだけが表示されます。ポリシーの表示を展開してポリシーを構成しているルールを表示するには、ポリシー名の左にある［+］ボタンをクリックします。展開したファイアウォール ポリシーの表示は、次のようになります。

		トラフィックの分類			アクション	ルール オプション
	ID	送信元	宛先	サービス		
	clients-servers-policy（クライアント対サーバ）					
	1	任意	任意	tcp	ファイアウォールの許可	
				udp		
				icmp		
	2	一致しないトラフィック			廃棄	

clients-servers-policy という名前のポリシーには、2 つの ACL が含まれています。ID 1 のルールでは、すべての送信元からすべての宛先への TCP、UDP、および ICMP トラフィックが許可されます。ID 2 のルールでは、一致しないトラフィックがすべて廃棄されます。

ポリシーへの新しいルールの追加

ポリシーに新しいルールを追加する手順は、次のとおりです。

ステップ 1　対象のポリシーの表示の任意の場所をクリックして、［+ 追加］ボタンをクリックします。

- 新しいトラフィックのルールを必要な順序で挿入するには、既存のルールを選択して［+ 追加］ボタンをクリックし、［挿入］または［下に挿入］を選択します。［挿入］および［下に挿入］オプションは、既存のルールを右クリックすると表示されるコンテキスト メニューからも選択できます。
- ［新しいトラフィックのルール］を選択すると、新しいルールが自動的にリストの先頭に配置されます。

- ［既存のトラフィックのルール］を選択すると、既存のクラス マップを選択して変更することができます。新しいルールは、自動的にリストの先頭に配置されます。

ステップ 2　表示されるダイアログで必要な操作を実行します。詳細については、「新しいルールの追加」を参照してください。

新しいゾーン ポリシーの追加

新しいゾーン ポリシーを追加するには、次の手順に従ってください。

ステップ 1　［追加］をクリックし、［新しいゾーン ポリシー］を選択します。

ステップ 2　［ルールの追加］画面で、［送信元ゾーン］フィールドの右側にあるボタンをクリックし、既存のゾーンを選択するか新しいゾーンを作成して、送信元ゾーンを指定します。

ステップ 3　［宛先ゾーン］フィールドの右側にあるボタンをクリックし、既存のゾーンを選択するか新しいゾーンを作成して、宛先ゾーンを指定します。

［ルールの追加］ウィンドウの他のフィールドの設定を行います。詳細については、「新しいルールの追加」を参照してください。

ポリシー内のルールの並べ替え

トラフィックを許可するルールがポリシーに複数含まれている場合は、ルールを選択して［上へ移動］ボタンまたは［下へ移動］ボタンをクリックすることによって、ルールの順序を変更できます。［上へ移動］ボタンは、すでにリストの先頭にあるルールを選択した場合、または一致しないトラフィック ルールを選択した場合は無効になります。［下へ移動］ボタンは、すでにリストの末尾にあるルールを選択した場合は無効になります。

［切り取り］および［貼り付け］ボタンを使用して、ルールの順序を変更することもできます。現在の位置からルールを削除するには、そのルールを選択して、［切り取り］をクリックします。新しい位置にルールを配置するには、既存のルールを選択して［貼り付け］をクリックし、［貼り付け］または［下に貼り付け］を選択します。

［上へ移動］、［下へ移動］、［切り取り］、［貼り付け］、および［下に貼り付け］の各操作は、ルールを右クリックすると表示されるコンテキスト メニューからも選択できます。

ルールのコピーと貼り付け

1 つのポリシーに含まれるルールをほとんど、あるいはまったく変更せずに別のポリシーで使用できる場合は、ルールのコピーと貼り付けを使用すると便利です。

ルールをコピーするには、そのルールを選択して［コピー］ボタンをクリックするか、ルールを右クリックして［コピー］を選択します。新しい位置にルールを貼り付けるには、［貼り付け］をクリックして、［貼り付け］または［下に貼り付け］を選択します。［貼り付け］および［下に貼り付け］ボタンは、コンテキスト メニューからも使用できます。新しい位置にルールを貼り付けると、［新しいルールの追加］ダイアログが表示され、必要に応じてそのルールを変更できます。

ルール フロー図の表示

ファイアウォール ポリシーの任意の場所をクリックして、［Rule Diagram］をクリックすると、そのポリシーのルール フロー図を表示できます。ルール フロー図では、ルータ アイコンの右に送信元ゾーンが、左に宛先ゾーンが表示されます。

変更の適用

変更をルータに送信するには、画面の下部にある［変更の適用］をクリックします。

変更の破棄

行った変更をルータに送信せずに破棄するには、画面の下部にある［変更の破棄］をクリックします。

新しいルールの追加

［ルールの追加］ウィンドウでトラフィック フローを定義し、検査するプロトコルを指定します。新しい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　ゾーン ポリシーを作成する場合は、［送信元ゾーン］フィールドと［宛先ゾーン］フィールドが表示されます。次の手順に従ってください。

a. 送信元ゾーンを指定するには、［送信元ゾーン］フィールドの横にあるボタンをクリックします。既存のゾーンを選択する場合は、［ゾーンの選択］をクリックし、表示されたダイアログでゾーンを選択します。ゾーンを作成する場合は、［ゾーンの作成］をクリックし、ゾーン名を入力して、表示されたダイアログでゾーンと関連付けるインターフェイスを指定します。

b. 宛先ゾーンを指定するには、［宛先ゾーン］フィールドの横にあるボタンをクリックします。既存のゾーンを選択する場合は、［ゾーンの選択］をクリックし、表示されたダイアログでゾーンを選択します。ゾーンを作成する場合は、［ゾーンの作成］をクリックし、ゾーン名を入力して、表示されたダイアログでゾーンと関連付けるインターフェイスを指定します。

ステップ 2　［送信元および宛先］フィールドで、トラフィックがネットワーク間を流れることを指定する場合は［ネットワーク］を選択し、トラフィックがエンティティ（ネットワークまたは個々のホスト）間を流れることを指定する場合は［任意］を選択します。

ステップ 3　［トラフィック名］フィールドにトラフィック フローの名前を入力します。

ステップ 4　［送信元ネットワーク］および［宛先ネットワーク］カラムの横にある［追加］をクリックして、送信元ネットワークおよび宛先ネットワークのアドレスを追加します。送信元ネットワークおよび宛先ネットワークとして、複数のエントリを追加できます。また、既存のエントリを選択して［編集］をクリックすると、既存のエントリを編集できます。

ステップ 5　必要に応じて、エントリを選択し、［上へ移動］または［下へ移動］をクリックして、エントリを並べ替えます。［上へ移動］ボタンは、選択したエントリがすでにリストの先頭にある場合は無効になります。［下へ移動］ボタンは、選択したエントリがすでにリストの末尾にある場合は無効になります。

ステップ 6　［サービス名］フィールドに、インスペクションの際に識別できるようにプロトコルまたはサービスを表す名前を入力します。

ステップ 7　サービスを指定するには、左側のカラムでツリーのブランチをクリックし、サービスを選択して、［追加 >>］をクリックします。ブランチの横の［+］アイコンをクリックすると、そのタイプの使用可能なサービスが表示されます。右側のカラムからサービスを削除するには、そのサービスを選択して、［<< 削除］をクリックします。

ステップ 8　［アクション］フィールドで［ファイアウォールの許可］、［ACL の許可］、または［廃棄］を選択して、トラフィックの処理方法を指定します。［ファイアウォールの許可］を選択した場合に、さらにアクション（［サービス］ボックスで選択したプロトコルのインスペクションなど）を定義するには、［詳細］をクリックしてメニュー項目を選択できます。詳細については、次のヘルプ トピックを参照してください。

- アプリケーション インスペクション
- URL フィルタ
- Quality of Service
- インスペクション パラメータ

ステップ 9　［廃棄］を選択した場合は、［ログ］をクリックして、イベントのログを記録できます。

ステップ 10　［OK］をクリックしてこのダイアログを閉じ、変更をルータに送信します。

トラフィックの追加

［トラフィックの追加］ダイアログを使用すると、ルールの送信元および宛先アドレスのエントリを作成できます。

アクション

［Include］または［Exclude］オプションを使用して、送信元アドレスと宛先アドレス間で交換されるトラフィックにルールを適用するかどうかを指定します。

対象のトラフィックをルールに含める場合は、［Include］を選択します。

対象のトラフィックをルールに含めない場合は、［Exclude］を選択します。

送信元ホスト / ネットワークおよび宛先ホスト / ネットワーク

次のフィールドに、トラフィックの送信元および宛先を指定します。

タイプ

次のいずれかの値を選択します。

- ［任意の IP アドレス］— トラフィックの送信元または宛先を任意のホストまたはネットワークに制限する場合に選択します。
- ［ネットワーク］— 送信元または宛先としてネットワーク アドレスを指定する場合に選択し、［IP アドレス］および［ワイルドカード マスク］フィールドにネットワーク アドレスを指定します。
- ［ホスト名または IP アドレス］— ホストの名前または IP アドレスを指定する場合に選択します。その後、［ホスト名 /IP］フィールドにホストを指定します。

IP アドレス

ネットワーク アドレスを入力します。このフィールドは、［タイプ］フィールドで［ネットワーク］を選択した場合に表示されます。

ワイルドカード マスク

ネットワーク アドレスに使用するビットを指定するワイルドカード マスクを入力します。たとえば、ネットワーク アドレスが 192.168.3.0 の場合は、マスクとして 0.0.0.255 と指定します。このフィールドは、［タイプ］フィールドで［ネットワーク］を選択した場合に表示されます。

ホスト名 /IP

このフィールドには、ホストの名前または IP アドレスを入力します。名前を入力する場合、ルータはその名前を IP アドレスに解決するために DNS サーバに接続できなければなりません。このフィールドは、［タイプ］フィールドで［ホスト名または IP アドレス］を選択した場合に表示されます。

アプリケーション インスペクション

この画面では、表示されているいずれかのアプリケーションまたはプロトコルの詳細パケット インスペクションを設定できます。これを実行するには、目的のアプリケーションまたはプロトコルの横にあるチェック ボックスを選択し、フィールドの右にあるボタンをクリックして、コンテキスト メニューから［作成］または［選択］を選択します。新しいポリシー マップを設定するには、［作成］を選択します。既存のポリシー マップをトラフィックに適用するには、［選択］を選択します。操作が完了すると、フィールドにポリシー マップ名が表示されます。

たとえば、インスタント メッセージングに新しいポリシー マップを作成するには、［IM］の横のチェック ボックスを選択し、［IM］フィールドの横のボタンをクリックして、［作成］を選択します。次に、［詳細パケット インスペクションの設定］ダイアログでポリシー マップを作成します。

URL フィルタ

［URL フィルタ名］リストから既存の URL フィルタを選択するか、または［新規作成］をクリックして、表示されるダイアログで URL フィルタを新規作成することによって、URL フィルタを追加します。このダイアログには、選択または作成した URL フィルタの設定の要約が表示されます。

Quality of Service

指定した秒速（ポリシング レート）を上回るトラフィック、および指定したバースト値を上回るトラフィックを破棄できます。ポリシング レートには毎秒 8,000 ～ 2,000,000,000 ビットの範囲の値を指定できます。バースト レートには 1,000 ～ 512,000,000 バイトの範囲の値を指定できます。

インスペクション パラメータ

［インスペクション パラメータ］ウィンドウでは、［インスペクション パラメータ マップ］リストからパラメータ マップを選択することによって、既存のパラメータ マップを指定するか、または［新規作成］をクリックして新しいパラメータ マップを作成して、変更するポリシーのルールに適用します。指定したパラメータ マップの詳細は、［プレビュー］ボックスに表示されます。

パラメータ マップについては、「インスペクション パラメータ マップと CBAC のタイムアウトおよびしきい値」を参照してください。

トラフィックの選択

ポリシーに追加するトラフィックを指定するクラス マップを選択します。特定のクラス マップの詳細を表示するには、そのクラス マップを選択して、［詳細の表示］をクリックします。

［OK］をクリックすると、選択したクラス マップの情報が示された［新しいルールの追加］ダイアログが表示されます。クラス マップは、変更を加えることも、変更せずにそのままにしておくこともできます。変更を加える場合に、元のクラス マップを使用する他のポリシーに変更が適用されないようにするには、クラス マップの名前を変更します。

削除ルール

このダイアログは、クラス マップまたは ACL が含まれるルールを削除するときに表示されます。クラス マップおよび ACL は、ルールと共に削除することも、他のルールで使用できるように保持することもできます。

このルールで使用していたクラス マップおよび ACL を自動的に削除する

このオプションは、対象のルールに含まれるクラス マップと ACL を削除する場合にクリックします。クラス マップと ACL はルータ設定から削除され、他のルールでも使用できなくなります。

使用していないクラス マップおよび ACL を後で削除する

このオプションは、クラス マップと ACL を保持したままルールだけを削除する場合にクリックします。クラス マップと ACL を保持しておき、ファイアウォール設定の他の部分で使用できます。

詳細の表示

削除対象のルールに関連付けられているクラス マップと ACL の名前を表示する場合は、［詳細の表示］をクリックします。ダイアログが開いて詳細が表示されます。［詳細の表示］をクリックすると、このボタン名は［詳細の非表示］に変わります。

詳細の非表示

このダイアログで詳細が表示されている部分を閉じる場合は、［詳細の非表示］をクリックします。［詳細の非表示］をクリックすると、このボタン名は［詳細の表示］に変わります。

クラス マップの手動削除

クラス マップを手動で削除するには、次の手順に従ってください。

ステップ 1　［設定］>［追加タスク］>［C3PL］>［クラス マップ］を選択します。

ステップ 2　削除するクラス マップのタイプを示すノードをクリックします。

ステップ 3　［詳細の表示］ウィンドウに表示されていたクラス マップの名前を選択して、［削除］をクリックします。

ACL の手動削除

ACL を手動で削除するには、次の手順に従ってください。

ステップ 1　［設定］>［追加タスク］>［ACL エディタ］を選択します。

ステップ 2　削除する ACL のタイプを示すノードをクリックします。

ステップ 3　［詳細の表示］ウィンドウに表示されていた ACL の名前または番号を選択して、［削除］をクリックします。