CHAPTER 33

ACL エディタ

ルールでは、特定の種類のトラフィックにルータがどのように対応するかを定義します。Cisco CP を使用すると、アクセス ルール、NAT ルール、および IPSec ルールを作成できます。アクセス ルールでは、ルータがブロックするトラフィック タイプと許可するトラフィック タイプを定義します。NAT ルールでは、アドレス変換の対象となるトラフィックを定義します。そして IPSec ルールでは、暗号化するトラフィックを指定します。Cisco CP には、ウィザードによる設定で使用されるデフォルト ルールも用意されています。このルールは、ユーザ独自のアクセス ルールを作成するときに調べたり使用したりできます。Cisco CP では、Cisco CP を使用して作成しなかったルール（外部ルールと呼ばれる）や Cisco SDM でサポートされていない構文を含むルール（サポートされていないルールと呼ばれる）も表示できます。

［ルール］画面では、ルータの設定のルールの概要を表示したり、他のウィンドウに移動してルールを作成、編集、または削除したりできます。

分類

ルールのタイプです。次のタイプがあります。

アクセス ルール	ネットワークのインバウンド トラフィックとアウトバウンド トラフィックを制御するルール。これらのルールは、ルータ インターフェイス、およびルータへのユーザのログオンを許可する VTY 回線で使用されます。

NAT ルール	プライベート IP アドレスを有効なインターネット IP アドレスに変換する方法を定義するルール
IPSec ルール	安全な接続上で暗号化するトラフィックを定義するルール
NAC ルール	ネットワークに対して許可される、またはネットワークからブロックされる IP アドレスを指定するルール
ファイアウォール ルール	送信元および宛先のアドレス、トラフィックのタイプ、およびトラフィックの許可または拒否を指定するルール
QoS ルール	ルールが関連付けられている QoS クラスに属する必要のあるトラフィックを指定するルール
サポートされていないルール	Cisco CP を使用せずに作成され、かつ Cisco CP でサポートされていないルール。これらのルールは読み取り専用であるため、Cisco CP で変更できません。
外部定義のルール	Cisco CP を使用せずに作成されたが、Cisco CP でサポートされているルール。これらのルールはどのインターフェイスにも関連付けられません。
Cisco CP デフォルト ルール	Cisco CP のウィザードで使用される定義済みのルールであり、［追加タスク］>［ACL エディタ］の順にクリックして表示されるウィンドウで適用できます。

ルールの数

このタイプのルールの番号です。

説明

ルールの説明が入力されている場合はそれが表示されます。

ルールを設定するには

ルール ツリーでルールのカテゴリをクリックし、そのルール タイプのウィンドウを表示します。そのウィンドウでルールを作成および編集します。

これらのウィンドウのヘルプ トピックには、実際に役立つ一般的な手順が記載されています。その他の操作の手順については、「アクセス ルールおよびファイアウォール関連の手順」を参照してください。

アクセス ルールおよびファイアウォール関連の手順

ここでは、実際に役立つ次のような手順について説明します。

- ファイアウォール上のアクティビティを表示する方法
- サポートされていないインターフェイス上でファイアウォールを設定する方法
- VPN を設定した後にファイアウォールを設定する方法
- 特定のトラフィックに DMZ インターフェイスの通過を許可する方法
- 新しいネットワークまたはホストからのトラフィックを許可するように既存のファイアウォールを変更する方法
- ファイアウォールに対して NAT パススルーを設定する方法
- Easy VPN コンセントレータへのトラフィックを、ファイアウォールを通過するように許可する方法
- ルールをインターフェイスに関連付ける方法
- アクセス ルールとインターフェイスの関連付けを解除する方法
- インターフェイスに関連付けられているルールを削除する方法
- Java リストのアクセス リストを作成する方法

ルール ウィンドウ

次のウィンドウでは、ルールを調査、作成、編集、および削除できます。

- ［アクセス ルール］ウィンドウ — アクセス ルールは、LAN へのインバウンドや LAN からのアウトバウンドを許可または拒否するトラフィックを定義するために最もよく使用されますが、それ以外の目的にも使用できます。
- ［NAT ルール］ウィンドウ — NAT ルールは、変換する一連のアドレスを指定するために使用されます。
- ［IPSec ルール］ウィンドウ — IPSec ルールは、VPN 接続で暗号化するトラフィックを指定するために IPSec ポリシーで使用される拡張ルールです。
- ［NAC ルール］ウィンドウ — ネットワークに対して許可される、またはネットワークからブロックされる IP アドレスを指定するルールです。
- ［ファイアウォール ルール］ウィンドウ — 送信元および宛先のアドレス、トラフィックのタイプ、およびトラフィックの許可または拒否を指定するルール
- ［QoS ルール］ウィンドウ — ルールが関連付けられている QoS クラスに属する必要のあるトラフィックを指定するルール
- ［サポートされていないルール］ウィンドウ — サポートされていないルールは、Cisco CP でサポートされていない構文またはキーワードを含むルールです。このルールは、ルータの動作に影響を及ぼす可能性がありますが、Cisco CP では読み取り専用になります。
- ［外部定義のルール］ウィンドウ — 外部定義のルールは、Cisco CP を使用せずに作成されたルールです。
- ［CCP デフォルト ルール］ウィンドウ — Cisco CP デフォルト ルールは、定義済みのアクセス ルールです。ウィザードによる最初の設定で使用され、ユーザが独自に設定を作成するときに使用できます。
- ［NAC ルール］ウィンドウ —NAC ルールは、NAC 検証プロセスで除外するホストを指定するために、NAC 例外ポリシーで使用されます。アドミッション コントロールでホストまたはネットワークを定義するためにも使用されます。

画面の上部には、このルータに設定されているアクセス ルールのリストが表示されます。このリストには、Cisco CP のデフォルト ルールは含まれません。Cisco CP のデフォルト ルールを表示するには、［ルール］ツリーの［SDM デフォルト ルール］ブランチをクリックします。

画面の下部には、選択したルールに関連付けられているルール エントリのリストが表示されます。ルール エントリは、インバウンド トラフィックまたはアウトバウンド トラフィックを照合する条件と、その条件に一致するトラフィックに対するアクションから構成されています。このボックス内のどのエントリの条件にも一致しないトラフィックは、廃棄されます。

最初のカラム

このカラムには、ルールのステータスを示すアイコンが表示されます。

 　ルールが読み取り専用の場合は、読み取り専用アイコンが表示されます。

名前 / 番号

アクセス ルールの名前または番号です。

標準アクセス リストは 1 ～ 99 の番号で識別されます。拡張アクセス リストは 100 ～ 199 の番号で識別されます。名前には英字を使用できるので、標準アクセス リストの範囲は 100 以上に、拡張アクセス リストの範囲は 200 以上に拡張できます。

使用元

このルールが適用されているインターフェイスの名前または VTY 番号です。

タイプ

ルールのタイプです。標準または拡張のどちらかです。

標準ルールでは、パケットの送信元 IP アドレスと IP アドレスの条件が照合され、一致するかどうかが調べられます。ルールの IP アドレスの条件には、1 つの IP アドレス全体を指定することも、IP アドレスの一部をワイルドカード マスクで指定することもできます。

拡張ルールを使用すると、パケットの送信元と宛先の IP アドレス、プロトコル タイプ、送信元と宛先のポート、その他のさまざまなパケット フィールドがルールと一致しているかどうかを調べることができます。

アクセス ルールは、標準ルールまたは拡張ルールとして定義できます。IPSec ルールは、サービス タイプを指定可能な、拡張ルールとして定義する必要があります。外部定義のルールとサポートされていないルールは、標準ルーとしても拡張ルールとしても定義できます。

説明

ルールの説明が入力されている場合はそれが表示されます。

最初のカラム（[ルール エントリ] エリア）

 　トラフィックを許可します。

 　トラフィックを拒否します。

アクション

このエントリの条件に一致するパケットがインターフェイスに到達したときに実行するアクション。値は［許可］または［拒否］です。

- ［許可］— このエントリの条件に一致するトラフィックを許可します。
- ［拒否］— このエントリの条件に一致するトラフィックを拒否します。

各ルール タイプにおける許可と拒否のアクションの詳細については、「キーワード「許可」と「拒否」の意味」を参照してください。

送信元

トラフィックが一致する必要のある送信元 IP アドレスの条件です。このカラムには、次のいずれかの値が含まれます。

- IP アドレスおよびワイルドカード マスク。IP アドレスでネットワークを指定し、ワイルドカード マスクで、ルールの IP アドレスがパケット内の IP アドレスとどの程度一致しなければならないかを指定します。

- キーワード「any」。「any」は、送信元 IP アドレスがどのような IP アドレスであってもかまわないことを示します。
- ホスト名。

宛先

拡張ルールの場合に、トラフィックが一致する必要のある宛先 IP アドレスの条件です。ネットワーク アドレス、または特定のホストのアドレスのいずれかです。このカラムには、次のいずれかの値が含まれます。

- IP アドレスおよびワイルドカード マスク。IP アドレスでネットワークを指定し、ワイルドカード マスクで、ルールの IP アドレスがパケット内の IP アドレスとどの程度一致しなければならないかを指定します。
- キーワード「any」。「any」は、送信元 IP アドレスがどのような IP アドレスであってもかまわないことを示します。
- ホスト名。

サービス

拡張ルールの場合、サービスでは、ルールと一致するパケットに含まれなければならないトラフィックのタイプを指定します。これは、echo-reply などのサービスの後に ICMP などのプロトコルが表示されて示されます。同じエンドポイント間の複数のサービスを許可または拒否するルールは、サービスごとに 1 つのエントリを含む必要があります。

属性

このフィールドには、このエントリに関するその他の情報（ロギングが有効になっているかどうかなど）を入力できます。

説明

エントリに関する簡単な説明です。

実行する操作

目的	手順
ルールを追加する。	［追加］ボタンをクリックし、表示されるウィンドウでルールを作成する。
ルールまたはルール エントリを編集する。	アクセス ルールを選択して［編集］をクリックする。表示される［ルールの編集］ウィンドウでルールを編集する。
ルールをインターフェイスに関連付ける。	「ルールをインターフェイスに関連付ける方法」を参照。
インターフェイスに関連付けられていないルールを削除する。	アクセス ルールを選択して［削除］をクリックする。
インターフェイスに関連付けられているルールを削除する。	Cisco CP では、インターフェイスに関連付けられているルールを削除できない。このようなルールを削除するには、まずルールとインターフェイスの関連付けを解除する必要がある。「インターフェイスに関連付けられているルールを削除する方法」を参照。
実行したい操作がここに記述されていない。	必要な操作の手順は、次のリンクを参照。アクセス ルールおよびファイアウォール関連の手順

ルールの追加 / 編集

このウィンドウでは、［ルール］ウィンドウで選択したルールを追加または編集できます。ルールの名前または番号の変更、ルール エントリの追加、変更、並べ替え、または削除、およびルールの説明の追加または変更を行うことができます。

名前 / 番号

ルールの名前または番号を追加または変更します。

標準ルールでは、1 ～ 99、または 1,300 ～ 1,999 の範囲内の番号を付ける必要があります。

拡張ルールでは、100 ～ 199 または 2,000 ～ 2,699 の範囲内の番号を付ける必要があります。

名前には英字を使用できるので、アクセス ルールに意味のあるラベルを関連付けることができます。

タイプ

追加するルールのタイプを選択します。標準ルールでは、パケット内の送信元ホストまたはネットワークがルータ上で調べられます。拡張ルールでは、送信元のホストまたはネットワーク、宛先のホストまたはネットワーク、およびパケットに含まれるトラフィックのタイプがルータ上で調べられます。

説明

このフィールドにはルールの説明を入力できます。説明の長さは 100 文字未満でなければなりません。

ルール エントリ リスト

このリストには、ルールを構成するエントリが表示されます。エントリは追加、編集、および削除できます。また、エントリを並べ替えて、評価される順序を変更することもできます。

ルール エントリを作成する際は、次のガイドラインを参照してください。

- リストには、許可のステートメントを少なくとも 1 つ含める必要があります。そうしなければすべてのトラフィックが拒否されます。
- すべてを許可またはすべてを拒否するエントリを一覧に含める場合は、リストの最後に置く必要があります。
- 標準エントリと拡張エントリを同じルール内に混在させることはできません。
- 同じルール内に重複するエントリが存在していてはなりません。

複製

このボタンをクリックすると、選択したエントリを新しいエントリのテンプレートとして使用できます。この機能を使用すると時間を節約でき、エラーを減らすことができます。たとえば、送信元と宛先が同じで、プロトコルまたはポートが異なる拡張ルール エントリを多数作成する場合は、まず［追加］ボタンを使用して最初のエントリを作成します。1 つめのエントリを作成したら、［複製］を使用してコピーし、プロトコル フィールドまたはポート フィールドを変更して新しいエントリを作成します。

インターフェイスの関連付け

ルールをインターフェイスに適用するには、［関連付け］ボタンをクリックします。

（注）　［関連付け］ボタンは、［アクセス ルール］ウィンドウからルールを追加する場合のみ有効です。

実行する操作

目的	手順
ルール エントリを追加または編集する。	［追加］をクリックし、表示されたウィンドウでエントリを作成する。または、［編集］をクリックし、表示されたウィンドウでエントリを変更する。
既存のエントリをテンプレートとしてルール エントリを追加する。	テンプレートとして使用するエントリを選択し、［複製］をクリックする。次に、表示されるダイアログ ボックスでエントリを作成する。 ダイアログ ボックスには、選択したエントリの内容が表示されるので、それを編集して新しいエントリを作成できる。
ルータによって特定のエントリが確実に評価されるようにルール エントリを並べ替える。	ルール エントリを選択し、［上へ移動］または［下へ移動］ボタンをクリックして、エントリを目的の位置に移動する。
ルールをインターフェイスに関連付ける。	［関連付け］をクリックし、［インターフェイスに関連付ける］ウィンドウでインターフェイスと方向を選択する。 ［関連付け］ボタンが有効になっていない場合は、［インターフェイスと接続］ウィンドウでインターフェイスをダブルクリックし、［関連付け］タブでルールをインターフェイスに関連付けることができる。
ルール エントリを削除する。	ルール エントリを選択し、［削除］をクリックする。表示される警告ウィンドウで、削除を確認する。

目的	手順
ルールについての理解を深める。	Cisco.com のリソースを参照する。次のリンクには、IP アクセス リストについての情報が含まれている。 http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml
実行したい操作がここに記述されていない。	必要な操作の手順は、次のリンクを参照。アクセス ルールおよびファイアウォール関連の手順

インターフェイスに関連付ける

このウィンドウでは、［アクセス ルール］ウィンドウで作成したルールをインターフェイスに関連付けたり、そのルールをアウトバウンド トラフィックとインバウンド トラフィックのどちらに適用するかを指定したりできます。

インターフェイスの選択

このルールを適用するインターフェイスを選択します。

方向の指定

インターフェイスへのインバウンド パケットがルータで確認されるようにする場合は、［インバウンド］をクリックします。ルータは、インバウンド パケットがルールに一致するかどうかを確認してからルーティングします。このとき、パケットは、ルールに許可と拒否のどちらのステートメントが含まれているかによって、受け入れられるか廃棄されます。パケットをアウトバウンド方向のインターフェイスに転送してからアクセス ルール内のエントリと照合する場合は、［アウトバウンド］をクリックします。

インターフェイスにすでに別のルールが関連付けられている場合

指定したインターフェイスと方向に別のアクセス ルールが関連付けられていることを知らせる情報ボックスが表示された場合は、操作をキャンセルするか、または続行できます。続行する場合は、インターフェイスにすでに適用されているルールにルール エントリを追加するか、またはインターフェイスとそのルールの関連付けを解除して新しいルールを関連付けます。

実行する操作

目的	手順
操作をキャンセルしてインターフェイスと既存のルールの関連付けを維持する。	［いいえ］をクリックする。既存のルールとインターフェイスの関連付けは維持され、［ルールの追加］ウィンドウで作成したルールは保存される。 既存のルールと新しいルールを調べて、既存のルールを新しいルールに置き換えるか、新しいルールのエントリを既存のルールにマージするかを決定できる。
操作を続行して、作成したルールのエントリを既存のルールにマージする。	［はい］をクリックする。既存のルールにマージするか既存のルールを置き換えるかを確認するウィンドウが表示されたら、［マージ］をクリックする。 新しいルール用に作成したエントリは、既存のルールの最後に追加される。 **（注）** マージするルールが既存のルールと互換性がない場合は、既存のルールを置き換えるしか方法はない。
操作を続行して、既存のルールを作成したルールに置き換える。	［はい］をクリックする。既存のルールにマージするか既存のルールを置き換えるかを確認するウィンドウが表示されたら、［置換］をクリックする。 置き換えられるルールは消去されない。インターフェイスおよび方向との関連付けが解除されるだけである。

標準ルール エントリの追加

標準ルール エントリでは、特定の送信元から送られたトラフィックを許可または拒否できます。送信元は、ネットワーク、または特定のネットワーク内のホストです。このウィンドウではルール エントリを 1 つ作成できますが、必要な場合はこのウィンドウに戻って、さらに多くのルール エントリを作成できます。

（注）　作成するいずれかのルール エントリの条件に一致しないトラフィックは、暗黙的に拒否されます。拒否するつもりがないトラフィックが確実に許可されるようにするには、設定するルールに明示的な許可エントリを追加する必要があります。

アクション

パケットがルール エントリの条件に一致したときにルータで実行されるようにするアクションを選択します。選択肢は［許可］と［拒否］です。これらのアクションによる処理は、そのアクションが使用されるルール タイプによって異なります。Cisco CP では、標準ルール エントリをアクセス ルール、NAT ルール、およびルート マップに関連付けられているアクセス リストで使用できます。各ルール タイプにおける許可と拒否のアクションの詳細については、「キーワード「許可」と「拒否」の意味」を参照してください。

送信元ホスト / ネットワーク

トラフィックが一致する必要のある送信元 IP アドレスの条件です。ウィンドウ内のこのエリアのフィールドは、［タイプ］フィールドの値に応じて変わります。

タイプ

次のいずれかを選択します。

- ネットワーク。そのアクションをネットワーク内のすべての IP アドレスに適用する場合に選択します。
- ホスト名または IP アドレス。そのアクションを特定のホストまたは IP アドレスに適用する場合に選択します。
- 任意の IP アドレス。そのアクションを任意の IP アドレスに適用する場合に選択します。

IP アドレス

［ネットワーク］を選択した場合、または［ホスト名または IP アドレス］を選択した場合は、このフィールドに IP アドレスを入力します。入力するアドレスがネットワーク アドレスの場合は、ワイルドカード マスクを入力して、ネットワーク アドレス内で一致している必要のある部分を指定します。

マスク

［ネットワーク］を選択した場合、または［ホスト名または IP アドレス］を選択した場合は、このリストからワイルドカード マスクを選択するか、カスタムのワイルドカード マスクを入力します。ワイルドカード マスク内の 2 進数の 0 は、パケットの IP アドレス内の対応するビットが正確に一致しなければならないことを意味します。ワイルドカード マスク内の 2 進数の 1 は、パケットの IP アドレス内の対応するビットが一致する必要がないことを意味します。

IP/ ホスト名

［タイプ］フィールドで［ホスト名または IP アドレス］を選択した場合は、ホストの名前または IP アドレスを入力します。ホスト名を入力する場合は、ルータが DNS サーバを使用するように設定されている必要があります。

説明

このフィールドには、エントリについての簡単な説明を入力できます。説明は、100 文字未満でなければなりません。

このエントリに一致した場合にログ

［システム プロパティ］でシスログ（Syslog）が指定されている場合は、このチェック ボックスを選択できます。選択すると、このエントリとの一致がシステム ログに記録されます。

拡張ルール エントリの追加

拡張ルール エントリでは、送信元と宛先、およびパケットで指定されているプロトコルとサービスに基づいて、トラフィックを許可または拒否できます。

（注）　作成するいずれかのルール エントリの条件に一致しないトラフィックは、暗黙的に拒否されます。拒否するつもりがないトラフィックが確実に許可されるようにするには、設定するルールに明示的な許可エントリを追加する必要があります。

アクション

パケットがルール エントリの条件に一致したときにルータで実行されるようにするアクションを選択します。選択肢は［許可］と［拒否］です。IPSec ルールのエントリを作成する場合の選択肢は、［トラフィックを保護する］および［トラフィックを保護しない］です。

これらのアクションによる処理は、そのアクションが使用されるルール タイプによって異なります。Cisco CP では、拡張ルール エントリを、アクセス ルール、NAT ルール、IPSec ルール、およびルート マップに関連付けられているアクセス リストで使用できます。各ルール タイプにおける許可と拒否のアクションの詳細については、「キーワード「許可」と「拒否」の意味」を参照してください。

送信元ホスト / ネットワーク

トラフィックが一致する必要のある送信元 IP アドレスの条件です。ウィンドウ内のこのエリアのフィールドは、［タイプ］フィールドの値に応じて変わります。

タイプ

次のいずれかを選択します。

- 特定の IP アドレス。これは、ネットワーク アドレス、または特定のホストのアドレスです。
- ホスト名。
- 任意の IP アドレス。

IP アドレス

［特定の IP アドレス］を選択した場合は、このフィールドに **IP アドレス**を入力します。入力するアドレスがネットワーク アドレスの場合は、ワイルドカード マスクを入力して、ネットワーク アドレス内で一致している必要のある部分を指定します。

マスク

［特定の IP アドレス］を選択した場合は、このリストからワイルドカード マスクを選択するか、カスタムのワイルドカード マスクを入力します。ワイルドカード マスク内の 2 進数の 0 は、パケットの IP アドレス内の対応するビットが正確に一致しなければならないことを意味します。ワイルドカード マスク内の 2 進数の 1 は、パケットの IP アドレス内の対応するビットが一致する必要がないことを意味します。

ホスト名

［タイプ］フィールドで［ホスト名］を選択した場合は、ホストの名前を入力します。

宛先ホスト / ネットワーク

トラフィックが一致する必要のある送信元 IP アドレスの条件です。ウィンドウ内のこのエリアのフィールドは、［タイプ］フィールドの値に応じて変わります。

タイプ

次のいずれかを選択します。

- 特定の IP アドレス。これは、ネットワーク アドレス、または特定のホストのアドレスです。
- ホスト名。
- 任意の IP アドレス。

マスク

［特定の IP アドレス］を選択した場合は、このリストからワイルドカード マスクを選択するか、カスタムのワイルドカード マスクを入力します。ワイルドカード マスク内の 2 進数の 0 は、パケットの IP アドレス内の対応するビットが正確に一致しなければならないことを意味します。ワイルドカード マスク内の 2 進数の 1 は、パケットの IP アドレス内の対応するビットが一致する必要がないことを意味します。

ホスト名

［タイプ］フィールドで［ホスト名］を選択した場合は、ホストの名前を入力します。

説明

このフィールドには、エントリについての簡単な説明を入力できます。説明は、100 文字未満でなければなりません。

プロトコルとサービス

エントリで適用するプロトコルおよびサービスがある場合はそれを選択します。入力する情報は、プロトコルごとに異なります。プロトコルをクリックすると、入力が必要な情報が表示されます。

送信元ポート

TCP または UDP が選択された場合に利用できます。このフィールドを設定すると、ルータによってパケットの送信元ポートにフィルタが適用されます。ただし、TCP 接続の送信元ポートの値の設定が必要になることはほとんどありません。このフィールドを使用するかどうかわからない場合は、「**= any**」のままにします。

宛先ポート

TCP または UDP が選択された場合に利用できます。このフィールドを設定すると、ルータによってパケットの宛先ポートにフィルタが適用されます。

選択するプロトコル	［送信元ポート］フィールドと［宛先ポート］フィールドで指定できる項目
TCP および UDP	送信元ポートと宛先ポートを名前または番号で指定する。名前または番号が思い出せない場合は、［...］ボタンをクリックして［サービス］ウィンドウから値を選択する。このフィールドには、0 ～ 65535 のプロトコル番号を指定できる。 • =. ルール エントリは、フィールドの右側に入力した値に適用される。 • !=. ルール エントリは、フィールドの右側に入力した値以外のすべての値に適用される。 • <. ルール エントリは、入力したポート番号より小さいすべてのポート番号に適用される。 • >. ルール エントリは、入力したポート番号より大きいすべてのポート番号に適用される。 • 範囲。エントリは、フィールドの右側で指定した範囲のポート番号に適用される。
ICMP	ICMP タイプとして［任意］を指定するか、タイプを名前か番号で指定する。名前または番号が思い出せない場合は、［...］ボタンをクリックして値を選択する。このフィールドには、0 ～ 255 のプロトコル番号を指定できる。
IP	IP プロトコルとして［任意］を指定するか、名前か番号でプロトコルを指定する。名前または番号が思い出せない場合は、［...］ボタンをクリックして値を選択する。このフィールドには、0 ～ 255 のプロトコル番号を指定できる。

Cisco CP で使用できるポート名とポート番号の表については、「サービスとポート」を参照してください。

このエントリに一致した場合にログ

ファイアウォール メッセージのロギングを設定してある場合は、このチェックボックスを選択できます。選択すると、シスログ（Syslog）サーバに送信されるログ ファイルに、このエントリとの一致が記録されます。詳細については、「ファイアウォール ログ」を参照してください。

ルールの選択

このウィンドウでは、使用するルールを選択します。

ルール カテゴリ

選択するルール カテゴリを選択します。選択したカテゴリ内のルールがリストの下のボックスに表示されます。ボックスにルールが表示されない場合、そのカテゴリにはまだルールが定義されていません。

名前 / 番号

ルールの名前または番号です。

使用元

ルールがどのように使用されるかを示します。たとえば、ルールがインターフェイスに関連付けられている場合は、そのインターフェイスの名前が表示されます。ルールが IPSec ポリシーで使用される場合は、そのポリシーの名前が表示されます。ルールが NAT によって使用される場合、このカラムには値 NAT が含まれます。

説明

ルールの説明です。

プレビュー

画面のこの領域には、選択したルールのエントリが表示されます。

アクション

［許可］または［拒否］のどちらかです。各ルール タイプにおける許可と拒否のアクションの詳細については、「キーワード「許可」と「拒否」の意味」を参照してください。

送信元

トラフィックが一致する必要のある送信元 IP アドレスの条件です。このカラムでは、次のことを指定できます。

- IP アドレスおよびワイルドカード マスク。IP アドレスでネットワークを指定し、ワイルドカード マスクで、ルールの IP アドレスがパケット内の IP アドレスとどの程度一致しなければならないかを指定します。
- キーワード「any」。「any」は、送信元 IP アドレスがどのような IP アドレスであってもかまわないことを示します。
- ホスト名。

宛先

拡張ルールの場合に、トラフィックが一致する必要のある宛先 IP アドレスの条件です。ネットワーク アドレス、または特定のホストのアドレスのいずれかです。このカラムでは、次のことを指定できます。

- IP アドレスおよびワイルドカード マスク。IP アドレスでネットワークを指定し、ワイルドカード マスクで、ルールの IP アドレスがパケット内の IP アドレスとどの程度一致しなければならないかを指定します。
- キーワード「any」。「any」は、送信元 IP アドレスがどのような IP アドレスであってもかまわないことを示します。
- ホスト名。

サービス

拡張ルールの場合、サービスでは、ルールと一致するパケットに含まれなければならないトラフィックのタイプを指定します。これは、echo-reply などのサービスの後に ICMP などのプロトコルが表示されて示されます。同じエンドポイント間の複数のサービスを許可または拒否するルールには、サービスごとに 1 つのエントリが含まれている必要があります。