



CHAPTER 34

Port-to-Application Mapping

Port-to-Application Mapping (PAM) を使用すると、ネットワーク サービスとアプリケーション用の TCP および UDP ポート番号をカスタマイズできます。PAM では、この情報を使用して、アプリケーションに関連付けられた登録済み（すなわち、既存）のポートとは異なるポートを使用するサービスを実行するネットワーク環境をサポートします。

PAM で保持される情報を使用することにより、コンテキストベース アクセス制御 (CBAC) でサポートされるサービスを非標準ポートで実行できるようになります。以前の CBAC では、アプリケーションに関連付けられた既存（すなわち、登録済み）のポートだけを使用してトラフィックを検査することしかできませんでした。現在、ネットワーク管理者は、PAM を使用して特定のアプリケーションやサービスのネットワーク アクセス コントロールをカスタマイズできます。

Port-to-Application Mapping

このウィンドウでは、ルータに設定されている Port-to-Application Mapping が表示され、PAM エントリを追加、編集、削除できます。ウィンドウの各行に、PAM エントリがタイプ別にグループ化されて表示されます。

追加 / 編集 / 削除ボタン

PAM エントリを作成、編集、削除する場合は、これらのボタンを使用します。[追加] ボタンをクリックすると、非標準ポート番号をプロトコル名にマップするエントリを作成できます。[編集] ボタンをクリックすると、ユーザ定義エントリを変更できます。[プロトコル タイプ] カラムにある システム定義 という値のエントリは、編集したり削除したりできません。

アプリケーション プロトコル カラム

このカラムには、アプリケーション プロトコル名とプロトコル タイプ名が表示されます。たとえば、FTP と TFTP の各エントリは、ファイル転送プロトコル タイプの下に表示されます。

ポート タイプ カラム

このリストは、ルータで Cisco IOS イメージが実行されている場合に表示されます。このイメージを使用して、このポート マップ エントリが TCP トラフィックまたは UDP トラフィックに適用されるかどうかを設定できます。

ポート カラム

このカラムには、ポート番号が表示されます。たとえば、HTTP のシステム定義エントリの場合、このカラムにはポート番号 80 が表示されます。HTTP のユーザ定義エントリの場合、このカラムにはポート番号 8080 あるいはカスタム定義番号が表示される可能性があります。

プロトコル タイプ カラム

このカラムの行には、次の値のいずれか 1 つが表示されます。

- **ユーザ定義** — エントリには、プロトコルとプロトコル番号間の非標準マッピングが含まれます。エントリは、アクセス コントロール リスト (ACL) で識別されるホスト IP アドレスと関連付けられている可能性があります。ACL の番号は、[アクセス リスト] カラムに表示されます。
- **システム定義** — エントリには、プロトコルとプロトコル番号間の標準の登録済みマッピング (*ftp 69* または *smtp 25* など) が含まれています。システム定義エントリは、編集、削除できません。システム定義エントリには、[アクセス リスト] カラム内の値は含まれません。システム定義エントリは、ネットワーク上の全ホストに適用されるためです。

アクセス リスト カラム

PAM エントリは、標準 ACL で定義されている単一ホストに適用されます。このカラムには、PAM エントリが適用されるホストの識別に使用する ACL の番号が表示されます。ホストを識別する ACL を参照する場合は、[設定] > [セキュリティ] > [ACL エディタ] > [アクセス ルール] を選択します。続いて、このウィンドウに表示された ACL 番号をクリックします。

説明カラム

PAM エントリの説明が作成されている場合、その説明がこのカラムに表示されます。

ポート マップ エントリの追加、編集

カスタムまたは標準プロトコルのポート マップ エントリを追加、編集できます。

プロトコル フィールド

エントリを追加する場合は、右側にあるリスト (...) ボタンをクリックし、システム定義プロトコルを選択することによって、あるいはカスタム プロトコルの名前を入力することによって、プロトコルを指定します。ポート マッピングがすでに存在しているカスタム定義プロトコル名は入力できません。

エントリーを編集する場合は、[プロトコル] フィールドは無効になります。プロトコルを変更する必要がある場合は、PAM エントリーを一度削除し、必要なプロトコル情報を指定して再度作成します。

説明フィールド

このフィールドは、ルータで Cisco IOS イメージが実行されている場合に表示されます。このイメージを使用して、このポート マップ エントリーが TCP または UDP トラフィックに適用されるかどうかを設定できます。ポート マップ エントリーの説明は任意に入力できます。説明は、カスタム プロトコルまたは特別なアプリケーションのエントリーを追加する場合に有用です。たとえば、ホスト sf-5 で実行している「orville」というカスタム データベース アプリケーションのエントリーを作成する場合は、「orville-sf-5」と入力します。

ポート タイプ リスト

このリストは、ルータで Cisco IOS イメージが実行されている場合に表示されます。このイメージを使用して、このポート マップ エントリーが TCP または UDP トラフィックに適用されるかどうかを設定できます。TCP または UDP を選択します。デフォルトは TCP です。

ポート番号フィールド

指定したプロトコルにマップするポート番号を入力します。ルータで Cisco IOS イメージ（このポート マップ エントリーが TCP または UDP トラフィックに適用されるかどうかを指定可能）が実行されている場合は、複数のポート番号をカンマで区切って指定するか、ダッシュで表されたポート番号範囲を入力することができます。たとえば、310, 313, 318 のように 3 つの非連続ポート番号を入力したり、415419 のように範囲を入力したりできます。

ルータで Cisco IOS イメージ（このポート マップ エントリーが TCP または UDP トラフィックに適用されるかどうかを指定可能）が実行されていない場合は、単一のポート番号を入力できます。

Host of Service フィールド

このポート マッピングが適用されるホストの IP アドレスを指定します。別のホストで同じマッピングが必要な場合は、そのポートに個別の PAM エントリーを作成します。