Security Device Manager： NBAR を使用した Cisco IOS ルータの P2P トラフィックのブロックの設定例

目次

概要

このドキュメントでは、Network Based Application Recognition（NBAR）を使用して、Cisco IOS® ルータが内部ネットワークからインターネットへのピアツーピア（P2P）トラフィックをブロックするように設定する方法について説明します。

NBAR は、ネットワークに使用される特定のネットワーク プロトコルとネットワーク アプリケーションを認識します。 NBAR によってプロトコルまたはアプリケーションが認識されると、モジュラ QoS コマンドライン インターフェイス（MQC）を使用して、そのプロトコルまたはアプリケーションに関連付けられているパケットをクラスにグループ化できます。 これらのクラスは、パケットが特定の基準に準拠しているかどうかに基づいてグループ化されます。

NBAR の場合は、NBAR に認識される特定のプロトコルまたはアプリケーションにパケットが一致するかどうかという基準になります。 MQC を使用すると、1 つのネットワーク プロトコル（citrix など）を使用するネットワーク トラフィックを 1 つのトラフィック クラスに配置し、異なるネットワーク プロトコル（gnutella など）に一致するトラフィックを別のトラフィック クラスに配置できます。 その後、各クラス内のネットワーク トラフィックには、トラフィック ポリ

シー（ポリシー マップ）を使用して適切な QoS 処理を適用できます。 NBAR の詳細については、『*Cisco IOS QoS ソリューション コンフィギュレーション ガイド*』（英語）の「NBAR を使用したネットワーク トラフィックの分類」セクション（英語）を参照してください。

前提条件

要件

NBAR が P2P トラフィックをブロックするように設定する前に、シスコ エクスプレス フォワーディング（CEF）を有効にする必要があります。

CEF を有効にするには、グローバル コンフィギュレーション モードで **ip cef** を使用します。

```
Hostname(config)#ip cef
```

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco 2801 ルータ（Cisco IOS® ソフトウェア リリース 12.4(15)T 搭載）
- Cisco Security Device Manager（SDM）バージョン 2.5

注: ルータを SDM で設定できるようにするには、『SDM を使用した基本的なルータ設定』を参照してください。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

Network-Based Application Recognition（NBAR）の概要

Network-Based Application Recognition（NBAR）は、多様なプロトコルとアプリケーションを認識および分類する分類エンジンです。 プロトコルまたはアプリケーションが NBAR に認識および分類されると、そのアプリケーションまたはそのプロトコルによるトラフィックに適した Quality of Service（QoS）を適用するようにネットワークを設定できるようになります。

NBAR は次の機能を実行します。

- **アプリケーションおよびプロトコルの識別（レイヤ 4 ～レイヤ 7）** NBAR では、次を使用するアプリケーションを分類できます。スタティックに割り当てられた伝送制御プロトコル（TCP）およびユーザ データグラム プロトコル（UDP）のポート番号。非 UDP および非 TCP IP プロトコル。接続の確立時にネゴシエートされる、動的に割り当てられた TCP および UDP のポート番号。 アプリケーションおよびプロトコルの分類には、ステートフル インスペクションが必要です。 ステートフル インスペクションは、割り当てが行われるデータ接続ポート上で制御接続を受け渡すことによって分類されるデータ接続を検出する機能です。

サブポート分類： 発行済みのアプリケーションの名前に基づいた、HTTP（URL、MIME またはホスト名）と Citrix アプリケーション Independent Computing Architecture（ICA）トラフィックの分類。ディープ パケット インスペクションと複数のアプリケーション固有の属性に基づいた分類。 リアルタイム転送プロトコル（RTP）のペイロード分類はこのアルゴリズムに基づいており、パケットは RTP ヘッダーの複数の属性に基づいて RTP として分類されます。

- **プロトコル ディスカバリ**プロトコル ディスカバリは一般的に使用される NBAR 機能で、インターフェイスごとにアプリケーションおよびプロトコルの統計情報（パケット数、バイト数、およびビット レート）を収集します。 GUI ベースの管理ツールは、NBAR PD 管理情報ベース（MIB）からの SNMP の統計をポーリングして、この情報をグラフィカルに表示します。 ネットワーキング機能と同様に、実稼働ネットワークにこの機能を導入する前にパフォーマンスとスケーラビリティの特性を理解することが重要です。 ソフトウェア ベースのプラットフォームで、この機能を有効にすると、CPU 使用率の低減と持続可能なデータ レートを実現します。 NBAR を、特定のインターフェイスの NBAR に対して既知であるすべてのプロトコルのトラフィックを検出するように設定するには、インターフェイス コンフィギュレーション モードまたは VLAN コンフィギュレーション モードで ip nbar protocol-discovery コマンドを使用します。 トラフィックの検出を無効にするには、**no ip nbar protocol-discovery コマンド**を使用します。

ピアツーピア（P2P）トラフィックのブロックの設定

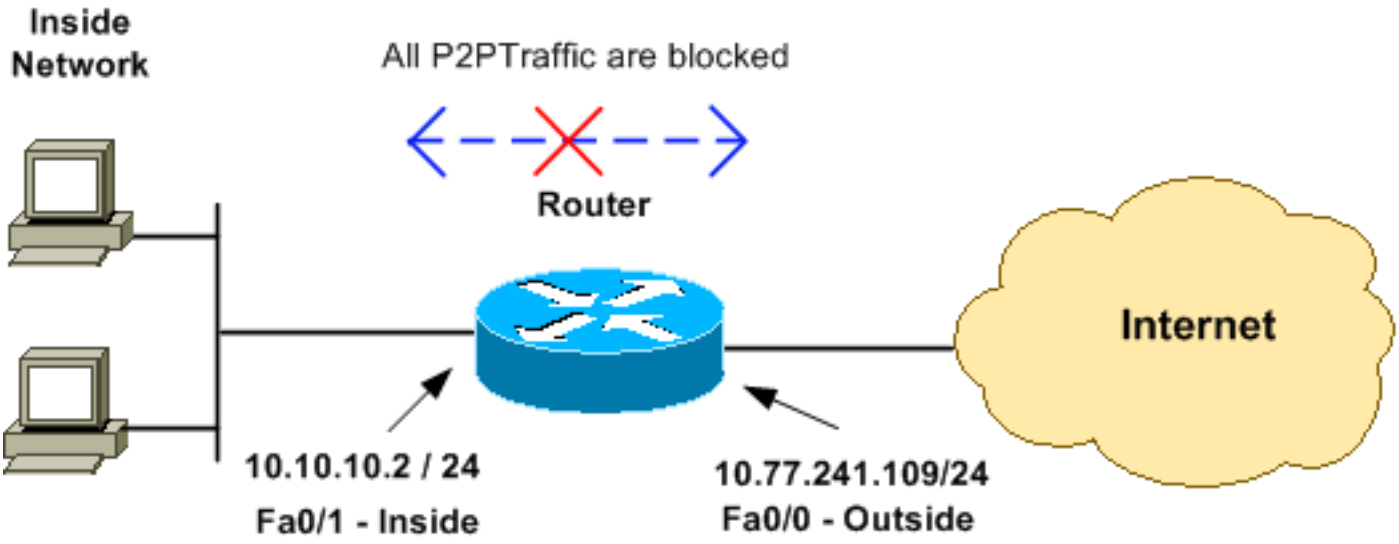
この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: 一部の P2P トラフィックは、その P2P プロトコルの特性のために完全にブロックされない場合があります。 これらの P2P プロトコルはそのシグニチャを動的に変更し、そのトラフィックを完全にブロックしようとする DPI エンジンをバイパスします。 そのため、それらを完全にブロックする代わりに帯域幅を制限することを推奨します （このトラフィックの帯域幅を絞ります。ただし、接続が維持される ぎりぎりの値にしてください）。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



ルータの設定

Cisco IOS ルータが P2P トラフィックをブロックするように設定する

```
R1#show run
Building configuration...

Current configuration : 4543 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
logging buffered 4096
enable secret 5 $1$bKq9$AHOxTgk6d3hcMGn6jTGxs/
!
aaa new-model
!
!
!
!
aaa session-id common
!--- IP CEF should be enabled at first to block P2P
traffic. !--- P2P traffic cannot be blocked when IPC CEF
is disabled. ip cef
!
!--- Configure the user name and password with Privilege
level 15 !--- to get full access when using SDM for
configuring the router. username cisco123 privilege 15
password 7 121A0C0411045D5679
secure boot-image
secure boot-config
archive
 log config
  hidekeys
!
!
!
!--- Configure the class map named p2p to match the P2P
protocols !--- to be blocked with this class map p2p.
```

```
class-map match-any p2p

!--- Mention the P2P protocols to be blocked in order to
block the !--- P2P traffic flow between the required
networks. edonkey, !--- fasttrack, gnutella, kazaa2,
skype are some of the P2P !--- protocols used for P2P
traffic flow. This example !--- blocks these protocols.
match protocol edonkey
 match protocol fasttrack
 match protocol gnutella
 match protocol kazaa2
 match protocol winmx
 match protocol skype

!--- The access list created is now mapped with the
class map P2P !--- to specify the interesting traffic.
match access-group 102
!
!
!--- Here the policy map named SDM-QoS-Policy-2 is
created, and the !--- configured class map p2p is
attached to this policy map. !--- Drop is the command to
block the P2P traffic.

policy-map SDM-QoS-Policy-2
 class p2p
   drop
!
!
!
!--- Below is the basic interface configuration on the
router. interface FastEthernet0/0 ip address
10.77.241.109 255.255.255.192 duplex auto speed auto !
interface FastEthernet0/1 ip address 10.10.10.2
255.255.255.0 !--- The command ip nbar protocol-
discovery enables NBAR !--- protocol discovery on this
interface where the QoS !--- policy configured is being
used.

 ip nbar protocol-discovery
 duplex auto
 speed auto
!--- Use the service-policy command to attach a policy
map to !--- an input interface so that the interface
uses this policy map.

 service-policy input SDM-QoS-Policy-2
!
ip route 10.77.241.0 255.255.255.0 10.10.10.2
ip route 10.77.0.0 255.255.0.0 10.77.241.65
!
!--- Configure the below commands to enable SDM !---
access to the Cisco routers. ip http server
ip http authentication local
no ip http secure-server
!
!--- Configure the access lists and map them to the
configured class map. !--- Here the access list 102 is
mapped to the class map p2p. The access !--- lists are
created for both Incoming and outgoing traffic through
!--- the inside network interface.

access-list 102 remark SDM_ACL Category=256
access-list 102 remark Outgoing Traffic
```

```
access-list 102 permit ip 10.10.10.0 0.0.0.255
10.77.241.0 0.0.0.255
access-list 102 remark Incoming Traffic
access-list 102 permit ip 10.77.241.0 0.0.0.255
10.10.10.0 0.0.0.255
!
!
line con 0
 exec-timeout 0 0
line aux 0
 password 7 02250C520807082E01165E41
line vty 0 4
 exec-timeout 0 0
 password 7 05080F1C22431F5B4A
 transport input all
!
!
webvpn cef
end
```

ルータへの SDM の設定

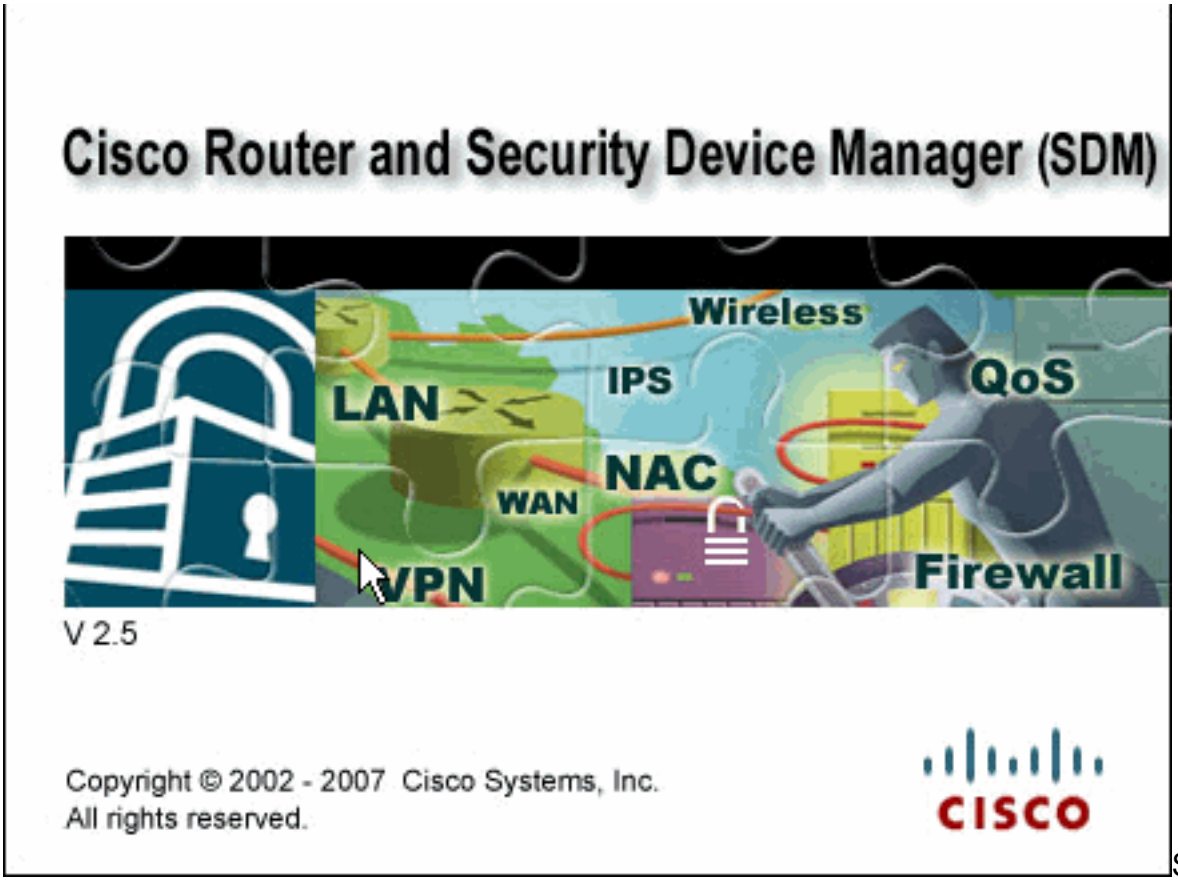
ルータ SDM の設定

Cisco IOS ルータが P2P トラフィックをブロックするように設定するには、次の手順を実行します。

注: NBAR を、特定のインターフェイスの NBAR に対して既知であるすべてのプロトコルのトラフィックを検出するように設定するには、インターフェイス コンフィギュレーション モードまたは VLAN コンフィギュレーション モードで ip nbar protocol-discovery コマンドを使用して、トラフィック ディスカバリを有効にする必要があります。 必要なインターフェイス (設定された QoS ポリシーを使用) 上でプロトコル ディスカバリを設定した後は、SDM 設定に進みます。

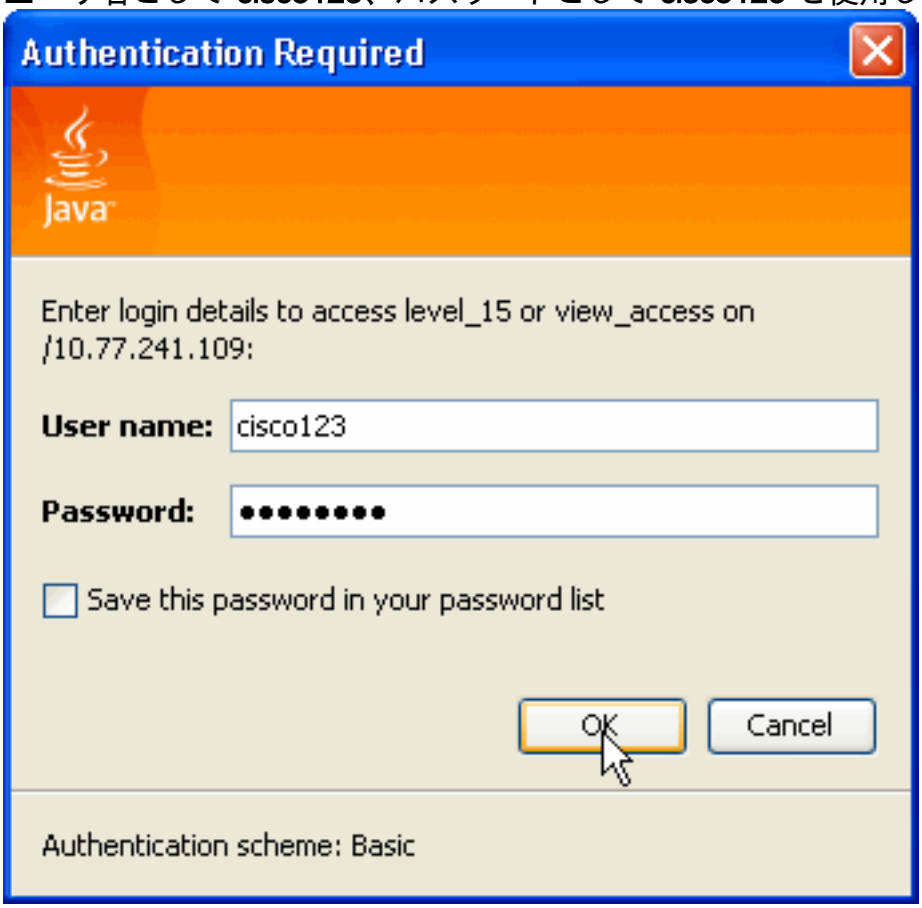
```
Hostname#config t
               Hostname(config)#interface fastEthernet 0/1
               Hostname(config-if)#ip nbar protocol-discovery
               Hostname(config-if)#end
```

1. ブラウザを開き、SDM アクセス用に設定されたルータの IP アドレスを入力します。 例：**https://<SDM_Router_IP_Address>**SSL 証明書の信憑性に関連してブラウザから出力されるすべての警告を認可します。 デフォルトのユーザ名とパスワードは、両方とも空白です。ルータがこのウィンドウを表示するのは、SDM アプリケーションのダウンロードを許可するためです。 次の例の場合、アプリケーションはローカル コンピュータにロードされ、Java アプレットでは動作しません。



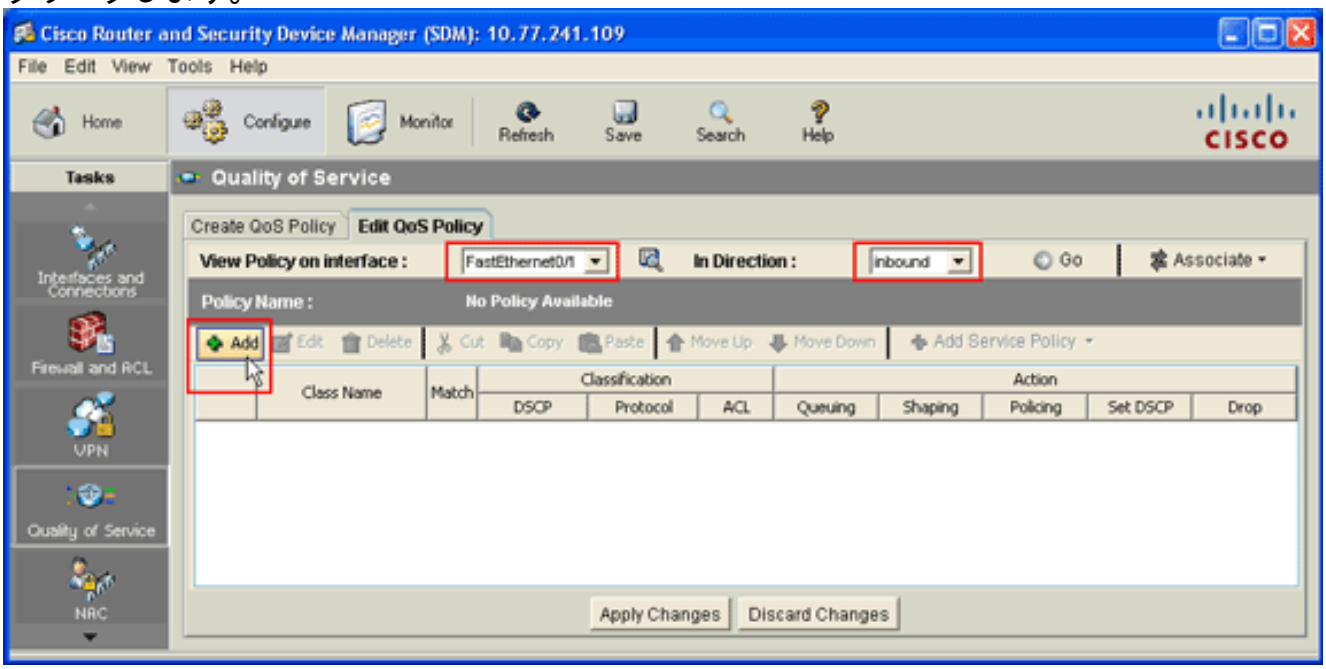
SDM のダウンロードが開始されます。

2. SDM Launcher がダウンロードされたら、ソフトウェアをインストールし、Cisco SDM Launcher を実行するために、プロンプトに従って一連の手順を完了します。
3. ユーザ名とパスワード（指定した場合）を入力し、[OK] をクリックします。次の例では、ユーザ名として **cisco123**、パスワードとして **cisco123** を使用しています。

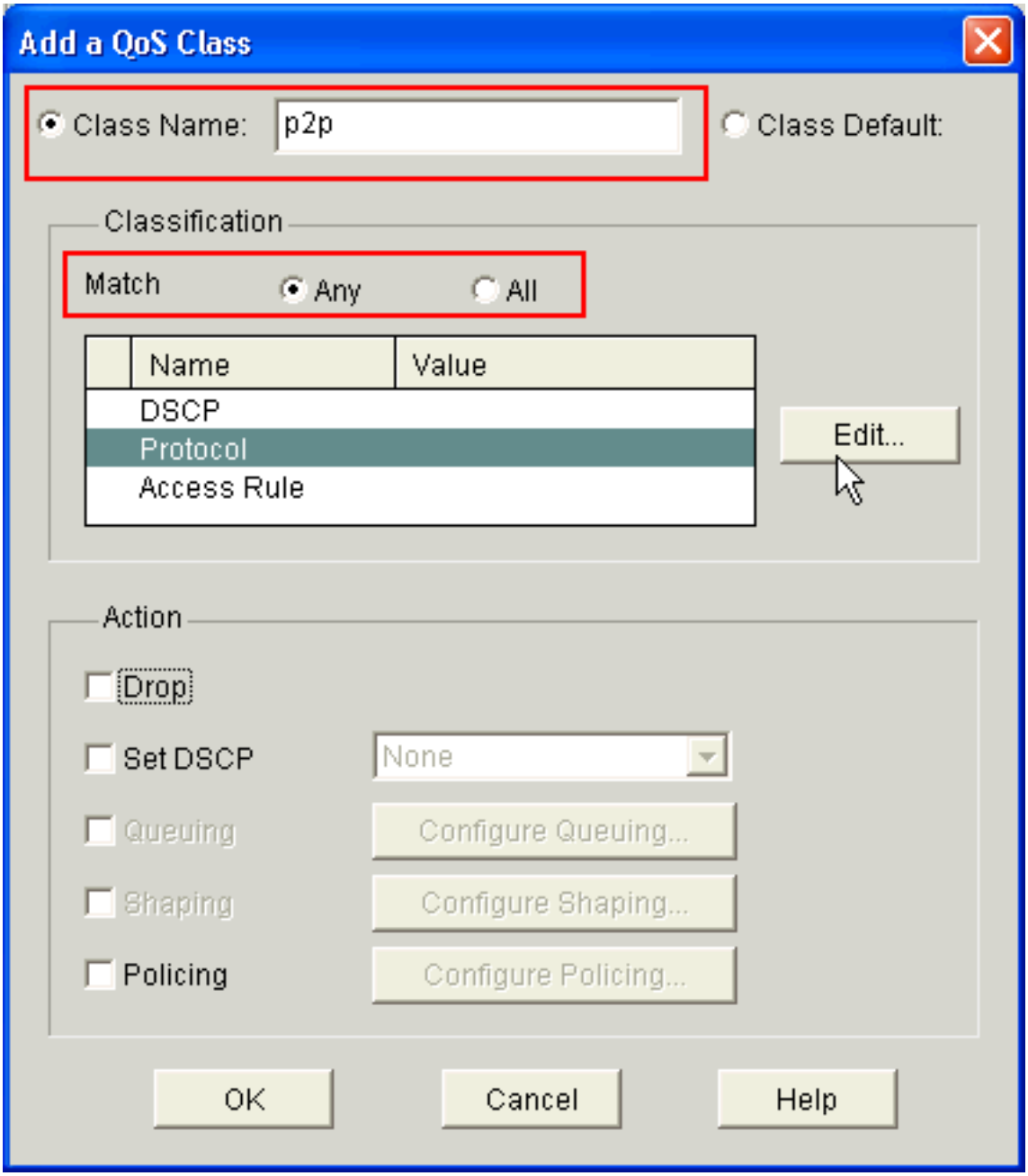


4. [Configure] > [Quality of Service] を選択し、SDM ホームページの [Edit QoS Policy] タブを

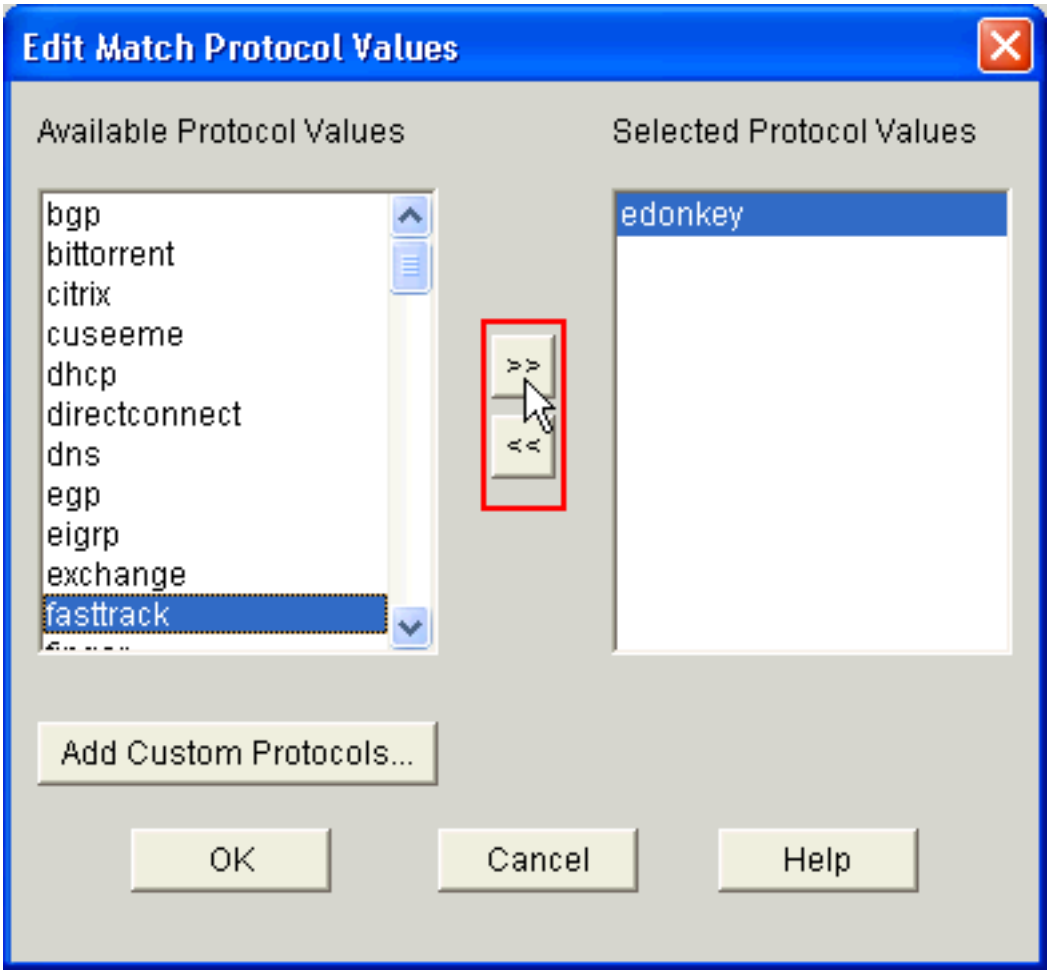
クリックします。



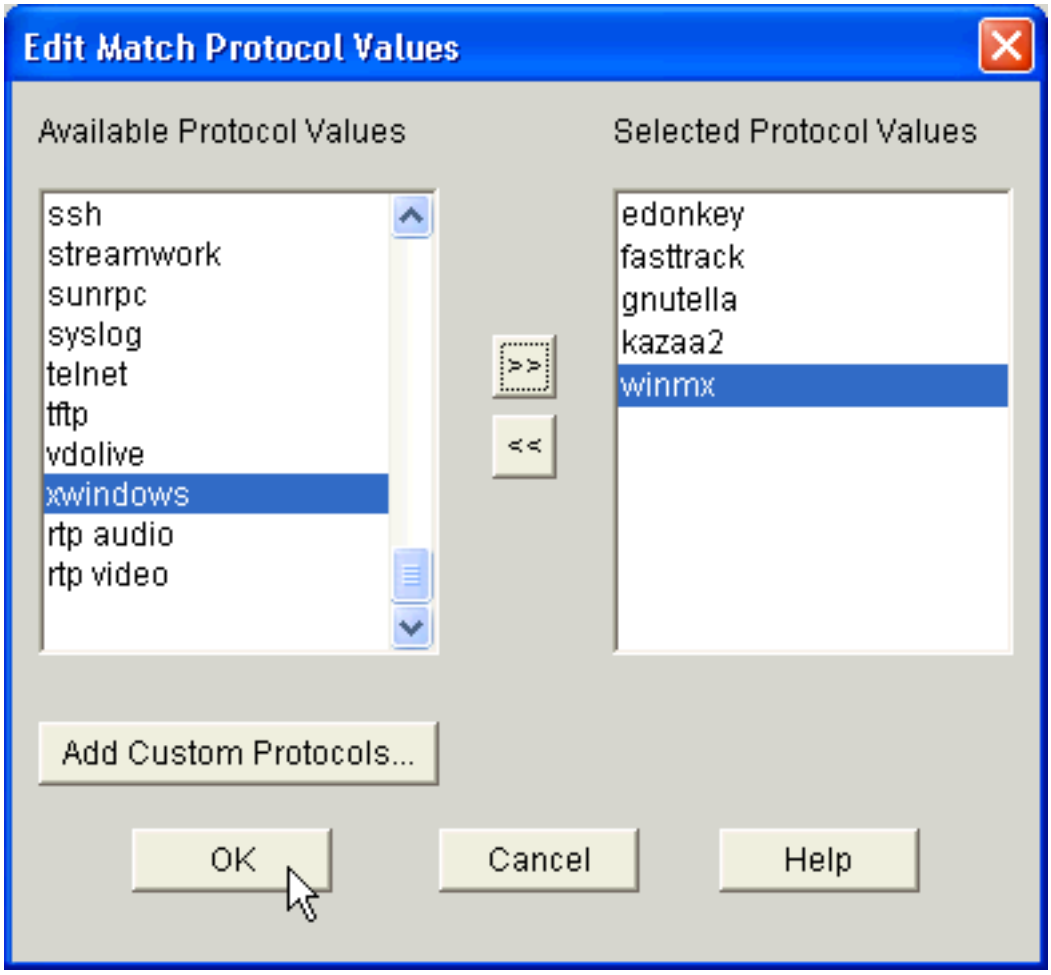
5. インターフェイスのドロップダウン リストの [View Policy] からインターフェイス名を選択し、次に [In Direction] ドロップダウン リストからトラフィック フローの方向（インバウンドまたはアウトバウンドのいずれか）を選択します。この例では、インターフェイスは [FastEthernet 0/1] で、方向は [inbound] です。
6. インターフェイスに新しい QoS クラスを追加するには、[Add] をクリックします。[Add a QoS Class] ダイアログボックスが表示されます。



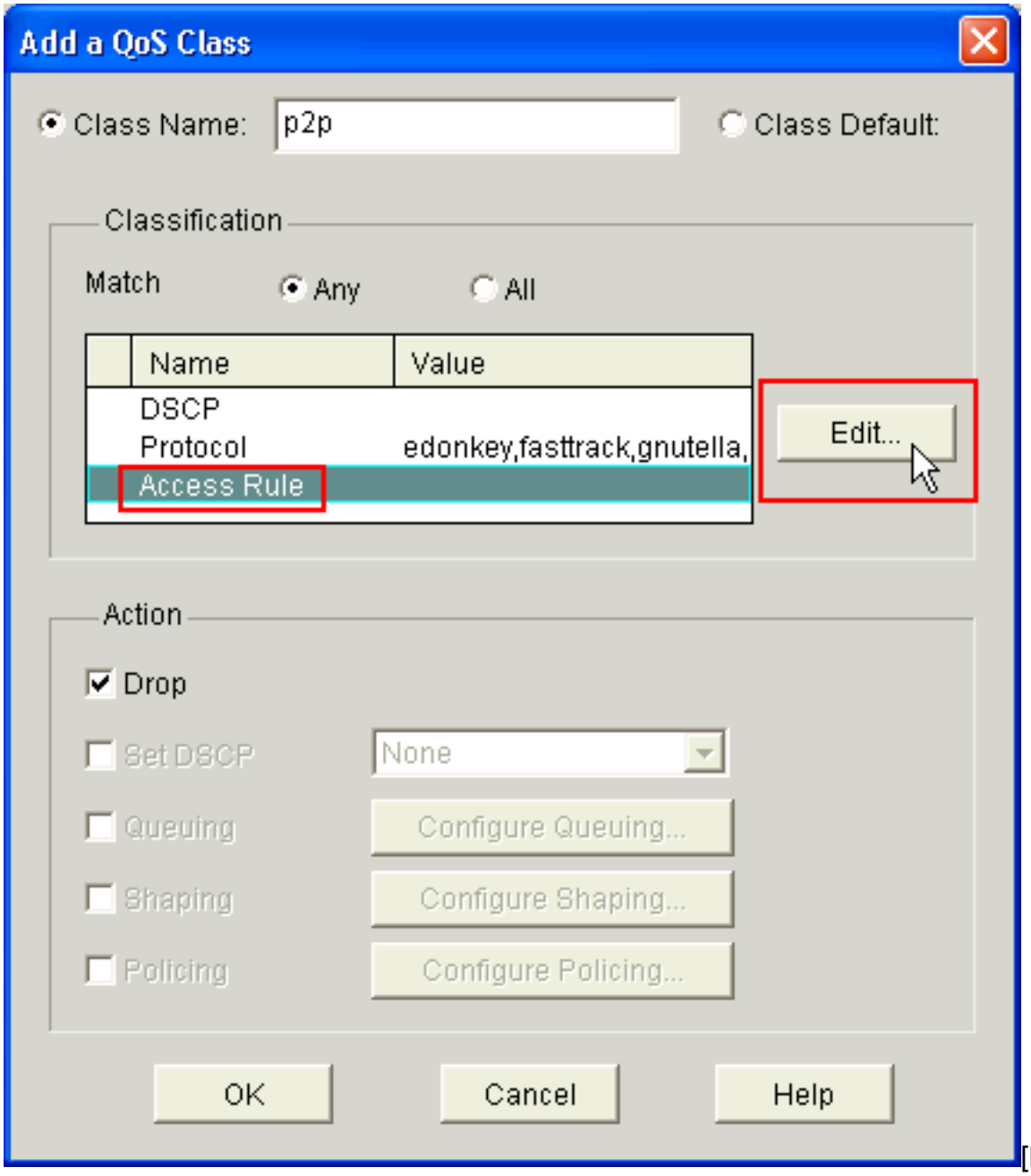
7. 新しいクラスを作成する場合は、[Class Name] オプション ボタンをクリックし、クラスの名前を入力します。 デフォルト クラスを使用する場合は、[Class Default] オプション ボタンをクリックします。この例では、*p2p* という名前の新しいクラスを作成します。
8. [Classification] 領域で、[Match] オプションの [Any] オプション ボタンまたは [All] オプション ボタンのいずれかをクリックします。この例では、ルータで class-map match-any p2p コマンドを実行する [Match] オプションは [Any] を使用しています。
9. [Classifcation] のリストで [Protocol] を選択し、[Edit] をクリックしてプロトコル パラメータを編集します。[Edit Match Protocol Values] ダイアログボックスが表示されます。



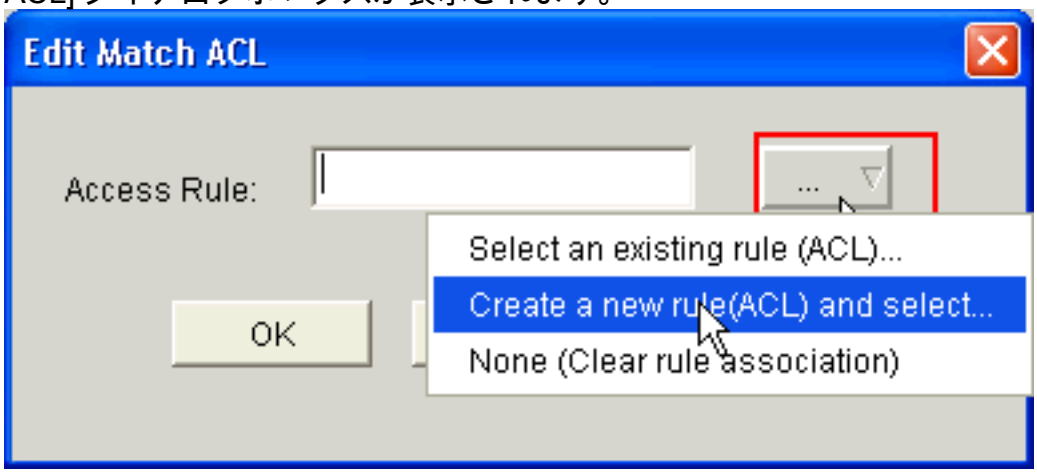
10. [Available Protocol Values] リストから、ブロックする各 P2P プロトコルを選択し、右矢印（**>>**）ボタンをクリックして各プロトコルを [Selected Protocol Values] リストに移動します。**注:** P2P トラフィックと NBAR を分類するには、Software Download ページに移動し、最新の P2P Protocol Description Language Module（PDLM）ソフトウェアと Readme ファイルをダウンロードします。 ダウンロードに使用できる P2P PDLM には、WinMx、Bittorrent、Kazaa2、Gnutella、eDonkey、Fasttrack、および Napster などがあります。 IOS によっては、これらの一部が統合されているものもあり（Fasttrack や Napster など）、最新の PDLM のバージョンを必要としない場合があります。 ダウンロードしたら、PDLM をルータのフラッシュにコピーし、**ip nbar pdlm <flash_device>: <filename>.pdlm** を設定して、それらを IOS にロードします。 正常にロードされたことを確認するには、**show ip nbar pdlm コマンド**を発行します。 ロードされた後は、クラス マップ コンフィギュレーションの下の match protocol 文でそれらを使用できます。
11. [OK] をクリックします。



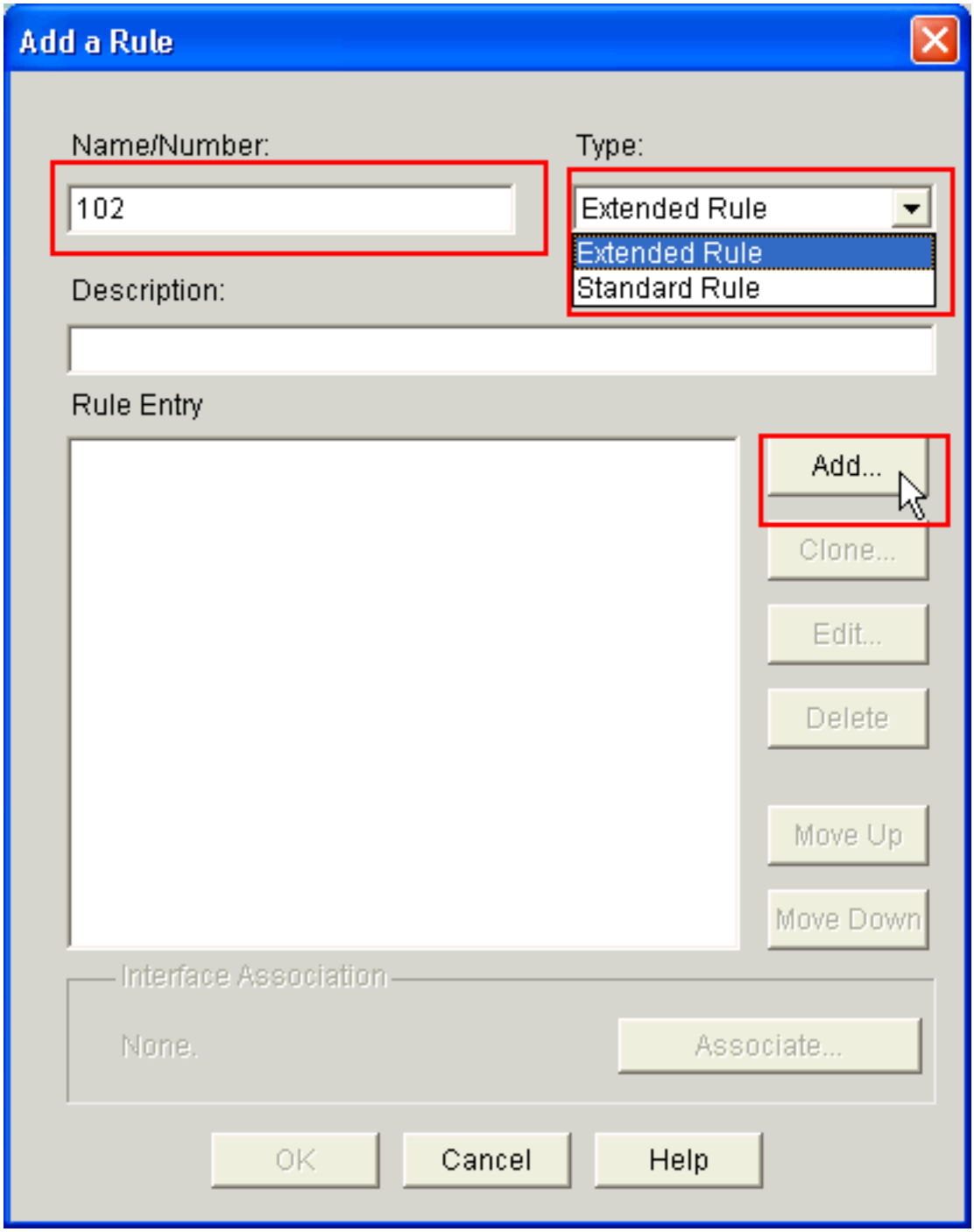
12. [Add a QoS Class] ダイアログボックスで、[Classification] リストから [Access Rules] を選択し、[Edit] をクリックして新しいアクセス ルールを作成します。 **p2p** クラス マップには既存のアクセス ルールをマッピングすることもできます。



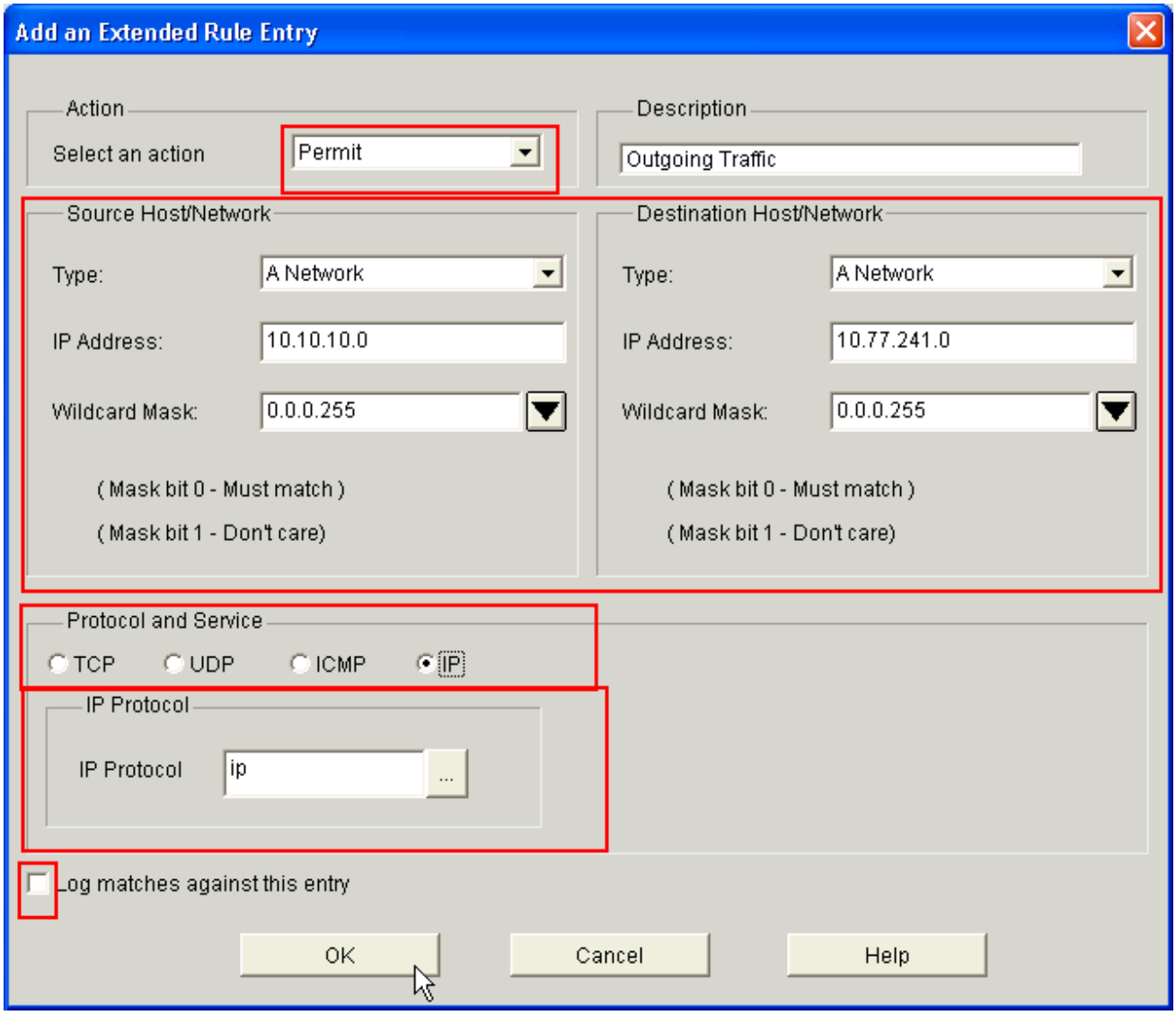
[Edit Match ACL] ダイアログボックスが表示されます。



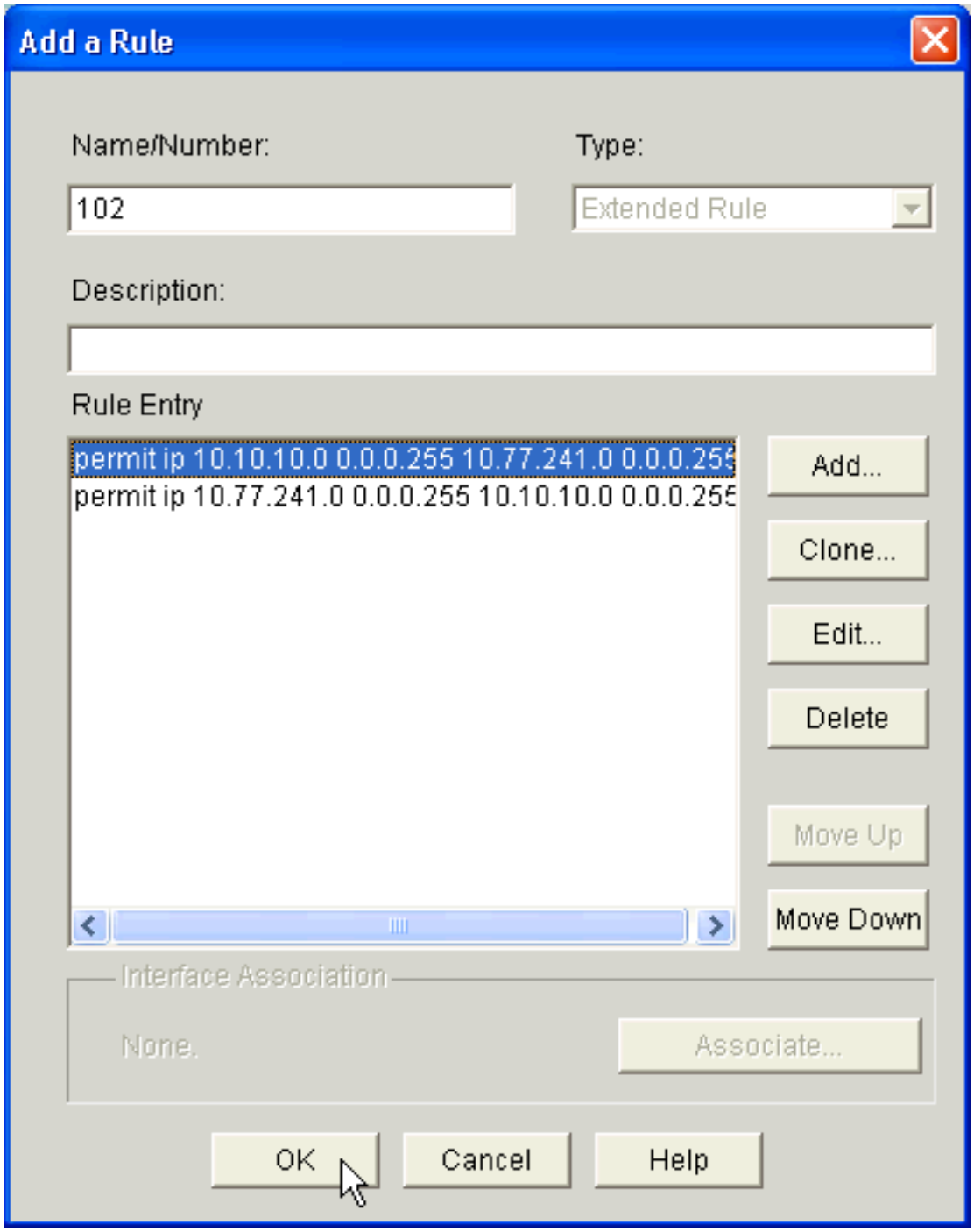
13. [Access Rule] ボタン (...) をクリックし、適切なオプションを選択します。 この例では、新しい ACL を作成します。[Add a Rule] ダイアログ ボックスが表示されます。



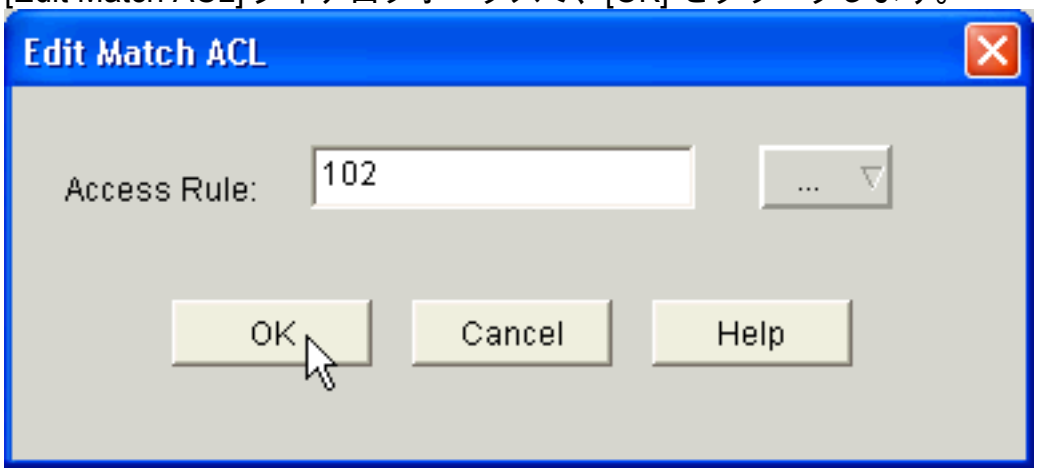
14. [Add a Rule] ダイアログボックスに、ACL の [Name/Number] フィールドに作成される ACL の名前または番号を入力します。
15. [Type] ドロップダウン リストから、作成する ACL のタイプを選択します（[Extended Rule] または [Standard Rule] のいずれか）。
16. [Add] をクリックして、ACL 102 に詳細を追加します。[Add an Extended Rule Entry] ダイアログボックスが表示されます。



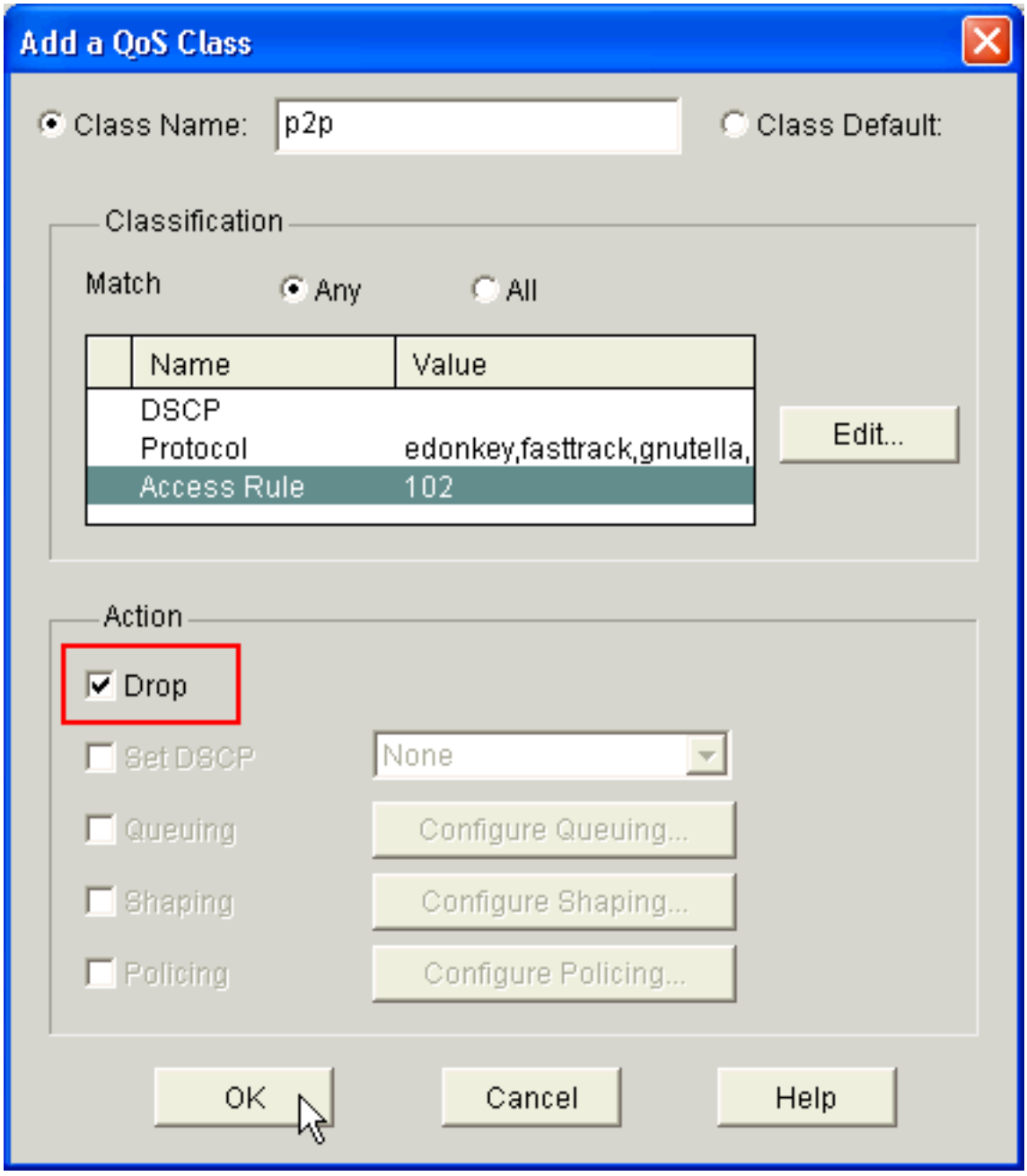
17. [Add an Extended Rule Entry] ダイアログボックスで、[Select an action] ドロップダウン リストからアクション ([Permit] または [Deny] のいずれか) を選択します。これにより、ACL ルールが、送信元と宛先のネットワーク間のトラフィックを許可するのか拒否するのかが決定されます。 このルールは、内部ネットワークから外部ネットワークへの発信トラフィックに適用されます。
18. [Source Host/Network] 領域および [Destination Host/Network] 領域にそれぞれ送信元および宛先ネットワークの情報を入力します。
19. [Protocol and Service] 領域で、適切なオプション ボタンをクリックします。 この例では IP を使用しています。
20. この ACL ルールに対する一致パケットを記録する場合は、[Log Matches against this entry] チェックボックスをオンにします。
21. [OK] をクリックします。
22. [Add a Rule] ダイアログボックスで、[OK] をクリックします。



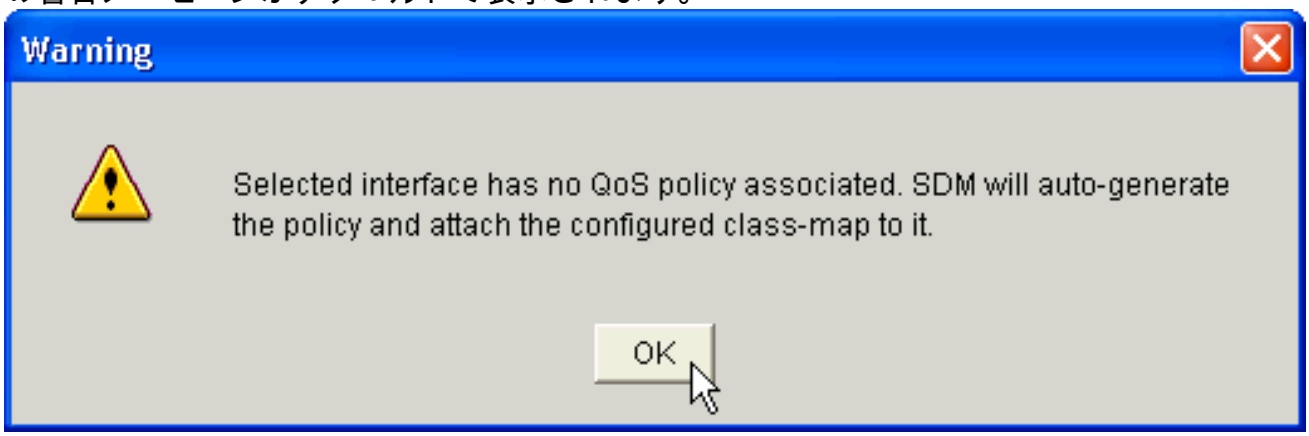
23. [Edit Match ACL] ダイアログボックスで、[OK] をクリックします。



24. [Add a QoS Class] ダイアログボックスで、[Drop] チェックボックスをオンにし、ルータが P2P トラフィックをブロックするよう強制します。



25. [OK] をクリックします。QoS ポリシーがインターフェイスにマッピングされないので、次の警告メッセージがデフォルトで表示されます。

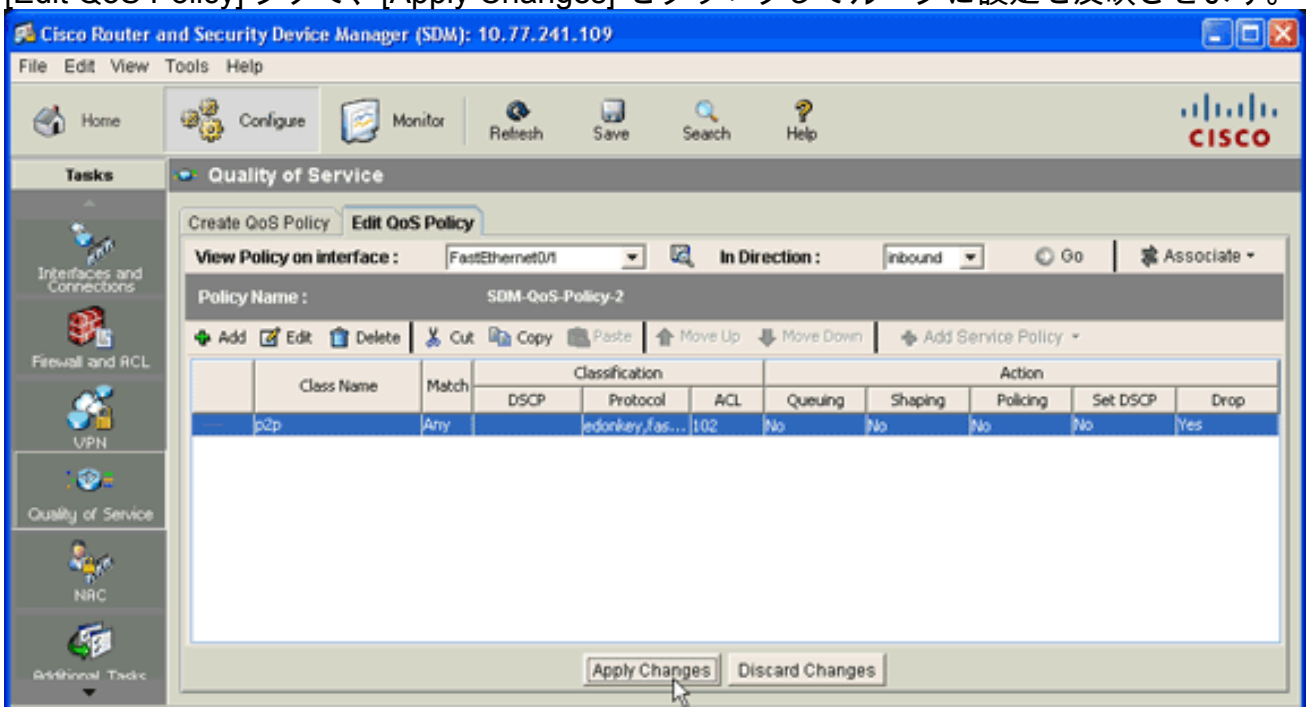


SDM は QoS ポリシーを自動的に生成し、設定されたクラス マップをポリシーに追加します。 この SDM の設定手順と同等のコマンドライン インターフェイス (CLI) は次のとおりです。

```
R1(config)#policy-map SDM-QoS-Policy-2
R1(config-pmap)#class p2p
R1(config-pmap-c)#drop
R1(config-pmap-c)#end
```

R1#

26. [Edit QoS Policy] タブで、[Apply Changes] をクリックしてルータに設定を反映させます。



アプリケーション ファイアウォール：Cisco IOS バージョン 12.4(4)T 以降のインスタント メッセージのトラフィック強制機能

インスタント メッセージのトラフィック強制

アプリケーション ファイアウォール：インスタント メッセージのトラフィック強制機能により、ネットワークで許可されるインスタント メッセンジャー トラフィックのタイプを特定するポリシーを定義および強制することができます。 application im の下の appfw policy に設定されている場合、複数のメッセンジャー（AOL、YAHOO、MSN など）を同時に制御できます。 そのため、次の追加機能も強制することができます。

- ファイアウォール インスペクション ルールの設定
- ペイロードのディープ パケット インスペクション（テキスト チャットなどのサービスを探す）

注: アプリケーション ファイアウォール：インスタント メッセージのトラフィック強制機能は Cisco IOS バージョン 12.4(4) 以降でサポートされています。

インスタント メッセンジャーのアプリケーション ポリシー

アプリケーション ファイアウォールは、アプリケーション ポリシー（スタティック シグニチャの集合で構成）を使用してセキュリティ違反を検出します。 スタティック シグニチャは、パラメータの集合で構成されます。このパラメータは、アクションを実行する前に満たす必要のあるプロトコル条件を指定します。 これらのプロトコル条件と応答は、CLI を介してアプリケーション ポリシーを形成するようにエンド ユーザによって定義されます。

Cisco IOS アプリケーション ファイアウォールは、インスタント ネイティブ メッセンジャー アプリケーション ポリシーをサポートするために拡張を続けてきました。 そのため、Cisco IOS フ

ァイアウォールは、AOL Instant Messenger（AIM）、Yahoo! Messenger、MSN Messenger のインスタント メッセージ サービス用のインスタント メッセンジャー サーバへのユーザによる接続を検出し、禁止できます。 この機能は、テキスト、音声、ビデオ、ファイル転送機能など、サポートされているすべてのサービスの接続を制御します。 この 3 つのアプリケーションは個別に拒否または許可することができます。 各サービスは、テキスト チャット サービスを許可して、音声、ファイル転送、ビデオ、およびその他のサービスを制限するなど、個別に制御できます。 この機能により、既存のアプリケーション インスペクション機能が向上し、HTTP（Web）トラフィックに偽装したインスタント メッセンジャー（IM）アプリケーション トラフィックを制御することができます。 詳細については、『アプリケーション ファイアウォール：インスタント メッセージのトラフィック強制』（英語）を参照してください。

注: IM アプリケーションがブロックされると、接続がリセットされ、必要に応じて syslog メッセージが生成されます。

確認

ここでは、設定が正常に動作していることを確認します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

- **show ip nbar pdlm：** 使用中の PDLM を NBAR によって表示するには、特権 EXEC モードで **show ip nbar pdlm コマンド**を使用します。`Router#show ip nbar pdlm`

```
The following PDLMs have been loaded:
flash://edonkey.pdlm
flash://fasttrack.pdlm
flash://gnutella.pdlm
flash://kazaa2.pdlm
```

- **show ip nbar version：** Cisco IOS リリースの NBAR ソフトウェアのバージョンまたは Cisco IOS ルータの NBAR PDLM のバージョンに関する情報を表示するには、特権 EXEC モードで **show ip nbar version コマンド**を使用します。`R1#show ip nbar version`

```
NBAR software version:  6

1   base                 Mv: 2
2   ftp                  Mv: 2
3   http                 Mv: 9
4   static               Mv: 6
5   tftp                 Mv: 1
6   exchange             Mv: 1
7   vdolive              Mv: 1
8   sqlnet               Mv: 1
9   rcmd                 Mv: 1
10  netshow              Mv: 1
11  sunrpc               Mv: 2
12  streamwork           Mv: 1
13  citrix               Mv: 10
14  fasttrack            Mv: 2
15  gnutella             Mv: 4
16  kazaa2               Mv: 7
17  custom-protocols     Mv: 1
18  rtsp                 Mv: 4
19  rtp                  Mv: 5
20  mgcp                 Mv: 2
21  skinny               Mv: 1
22  h323                 Mv: 1
23  sip                  Mv: 1
```

```
24  rtcp                Mv: 2
25  edonkey             Mv: 5
26  winmx               Mv: 3
27  bittorrent          Mv: 4
28  directconnect       Mv: 2
29  skype               Mv: 1


{<No.>}<PDLM name> Mv: <PDLM Version>, {Nv: <NBAR Software Version>; <File name>
}{Iv: <PDLM Interdependency Name>   - <PDLM Interdependency Version>}
```

- show policy-map interface：特定のインターフェイスまたはサブインターフェイスまたはインターフェイス上の特定の相手先固定回線接続（PVC）のいずれかのすべてのサービス ポリシーに設定されたすべてのクラスのパケット統計情報を表示するには、特権 EXEC モードで **show policy-map interface コマンド**を使用します。`R1#show policy-map interface fastEthernet 0/1`

```
 FastEthernet0/1

  Service-policy input: SDM-QoS-Policy-2

    Class-map: p2p (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol edonkey
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol fasttrack
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol gnutella
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol kazaa2
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol winmx
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: access-group 102
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol skype
        0 packets, 0 bytes
        5 minute rate 0 bps
      drop

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

- **show running-config policy-map**：すべてのポリシー マップ コンフィギュレーション、またはデフォルトのポリシー マップ コンフィギュレーションを表示するには、**show running-config policy-map コマンド**を使用します。`R1#show running-config policy-map`

```
Building configuration...

Current configuration : 57 bytes
!
policy-map SDM-QoS-Policy-2
 class p2p
   drop
!
end
```

- **show running-config class-map**：クラス マップ コンフィギュレーションに関する情報を表示するには、**show running-config class-map コマンド**を使用します。`R1#show running-config class-map`

```
Building configuration...

Current configuration : 178 bytes
!
class-map match-any p2p
 match protocol edonkey
 match protocol fasttrack
 match protocol gnutella
 match protocol kazaa2
 match protocol winmx
 match access-group 102
!
end
```

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

注: debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

- **show access-list**：Cisco IOS ルータで稼働するアクセスリスト コンフィギュレーションを表示するには、**show access-list コマンド**を使用します。`R1#show access-lists`

```
Extended IP access list 102
    10 permit ip 10.10.10.0 0.0.0.255 10.77.241.0 0.0.0.255
    20 permit ip 10.77.241.0 0.0.0.255 10.10.10.0 0.0.0.255
```

関連情報

- 『Cisco IOS セキュリティ設定ガイド、リリース 12.4』
- Network-Based Application Recognition（NBAR）
- Cisco Express Forwarding（CEF）
- テクニカルサポートとドキュメント - Cisco Systems