مدير جهاز الأمان: حظر حركة مرور البيانات عبر بروتوكول P2P على موجه Cisco IOS باستخدام مثال تكوين NBAR

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين موجه Cisco IOS® لحظر حركة مرور نظير إلى نظير (P2P) من الشبكة الداخلية إلى الإنترنت باستخدام التعرف على التطبيق المستند إلى الشبكة (NBAR).

يتعرف NBAR على بروتوكولات شبكة معينة وتطبيقات شبكة تستخدم في شبكتك. وبمجرد التعرف على بروتوكول أو تطبيق من قبل NBAR، يمكنك إستخدام واجهة سطر أوامر جودة الخدمة النمطية (MQC) لتجميع الحزم المرتبطة بتلك البروتوكولات أو التطبيقات في فئات. يتم تجميع هذه الفئات على أساس ما إذا كانت الحزم تتوافق مع معايير معينة أم لا.

ل NBAR، المعيار هو ما إذا كانت الحزمة تطابق بروتوكول معين أو تطبيق معروف ل NBAR. باستخدام MQC، يمكن وضع حركة مرور الشبكة باستخدام بروتوكول شبكة واحد (Citrix، على سبيل المثال) في فئة حركة مرور واحدة، بينما يمكن وضع حركة المرور التي تطابق بروتوكول شبكة مختلف (gnutella، على سبيل المثال) في فئة حركة مرور أخرى. وفيما بعد، يمكن منح حركة مرور الشبكة داخل كل فئة المعالجة المناسبة لجودة الخدمة باستخدام سياسة حركة مرور البيانات (خريطة السياسة). راجع قسم تصنيف حركة مرور الشبكة باستخدام شريط الإنترنت من *دليل تكوين حلول جودة الخدمة من Cisco IOS* للحصول على مزيد من المعلومات حول NBAR.

المتطلبات الأساسية

المتطلبات

قبل تكوين NBAR لحظر حركة مرور P2P، يجب تمكين إعادة التوجيه السريع من Cisco (CEF).

أستخدم **ip cef** في وضع التكوين العام لتمكين CEF:

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

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- cisco 2801 مسحاج تخديد مع cisco ios ® برمجية إطلاق T(15)12.4
- Cisco Security Device Manager (SDM)، الإصدار 2.5

ملاحظة: ارجع إلى تكوين الموجه الأساسي باستخدام SDM للسماح بتكوين الموجه بواسطة SDM.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

نظرة عامة على التعرف على التطبيق المستند إلى الشبكة (NBAR)

التعرف على التطبيق المستند إلى الشبكة (NBAR) هو محرك تصنيف يقوم بالتعرف على مجموعة كبيرة من البروتوكولات والتطبيقات وتصنيفها. عندما يتعرف NBAR على بروتوكول أو تطبيق وتصنيفه، يمكن تكوين الشبكة لتطبيق جودة الخدمة (QoS) المناسبة لذلك التطبيق أو حركة المرور مع ذلك البروتوكول.

ينجز NBAR هذه الدوال:

- **تعريف التطبيقات والبروتوكولات (من الطبقة الرابعة إلى الطبقة السابعة)**يمكن أن تصنف NBAR التطبيقات التي تستخدم:أرقام منافذ بروتوكول التحكم في النقل (TCP) المعين بشكل ثابت وبروتوكول مخطط بيانات المستخدم (UDP).بروتوكولات IP بخلاف UDP والبروتوكولات بخلاف TCP.تم التفاوض على أرقام منافذ TCP و UDP المعينة ديناميكيا أثناء إنشاء الاتصال. يلزم إجراء فحص يحدد الحالة لتصنيف التطبيقات والبروتوكولات. يقصد ب State Inspection القدرة على اكتشاف إتصالات البيانات التي سيتم تصنيفها عن طريق تمرير إتصالات التحكم عبر منفذ اتصال البيانات حيث يتم إجراء التعيينات.تصنيف المنفذ الفرعي: تصنيف حركة مرور بيانات HTTP (عناوين URL أو MIME أو أسماء الأجهزة المضيفة) وبنية Citrix Applications Independent Computing Architecture (ICA) استنادا إلى اسم التطبيق المنشور.التصنيف استنادا إلى الفحص العميق للحزم والسمات المتعددة الخاصة بالتطبيق. يستند تصنيف حمولة بروتوكول نقل الوقت الفعلي (RTP) إلى هذه الخوارزمية التي يتم فيها تصنيف الحزمة إلى RTP استنادا إلى سمات متعددة في رأس RTP.
- **اكتشاف البروتوكول**اكتشاف البروتوكول هو ميزة NBAR شائعة الاستخدام تقوم بتجميع إحصائيات التطبيق والبروتوكول (عدد الحزم وعدد وحدات البايت ومعدلات وحدات البت) لكل واجهة. ويمكن لأدوات الإدارة المستندة إلى واجهة المستخدم الرسومية عرض هذه المعلومات بيانيا، من خلال إحصائيات SNMP الخاصة بالاقتراع من

قاعدة معلومات إدارة MIB (NBAR PD). كما هو الحال مع أي ميزة شبكة، من المهم فهم خصائص الأداء وقابلية التوسع قبل نشر الميزة في شبكة إنتاج. في الأنظمة الأساسية المستندة إلى البرامج، تكون المقاييس التي يتم مراعاتها هي تأثير إستخدام وحدة المعالجة المركزية (CPU) ومعدل البيانات المستدام أثناء تمكين هذه الميزة. in order to شكلت NBAR أن يكتشف حركة مرور لكل بروتوكول أن يكون معروف أن nbar على قارن خاص، يستعمل ال ip nbar protocol-discovery أمر في قارن تشكيل أسلوب أو VLAN تشكيل أسلوب.
لتعطيل اكتشاف حركة المرور، أستخدم الأمر **no ip nbar protocol-discovery**.

تكوين حظر حركة مرور نظير إلى نظير (P2P)

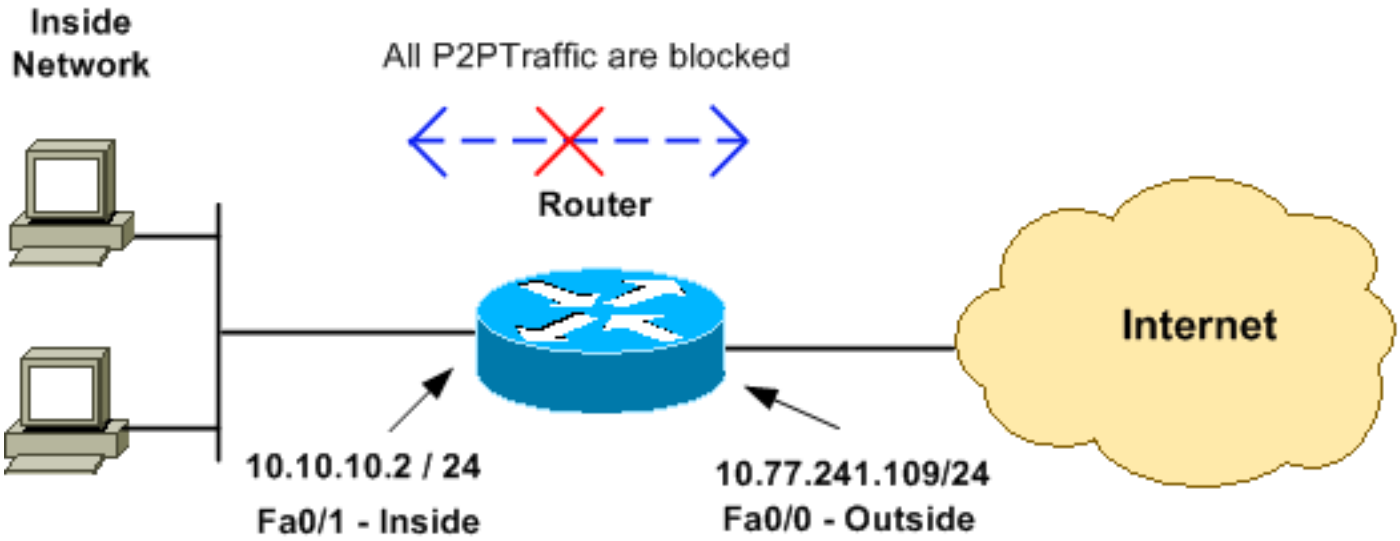
في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: لا يمكن حظر بعض حركة مرور P2P بشكل كامل بسبب طبيعة بروتوكول P2P الخاص بها. تعمل بروتوكولات P2P هذه على تغيير تواقيعها بشكل ديناميكي لتخطي أي محركات DPI تحاول حظر حركة مرور البيانات الخاصة بها بشكل كامل. لذلك، توصي Cisco بتقييد النطاق الترددي بدلا من حظرها بالكامل. (كبح النطاق الترددي لحركة المرور هذه. امنح عرض نطاق ترددي أقل للغاية، ومع ذلك، دع الاتصال يمر.)

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



تكوين الموجّه

التكوين لحظر حركة مرور البيانات عبر بروتوكول P2P على موجه Cisco IOS
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
```

تكوين الموجه باستخدام SDM

تكوين SDM للموجه

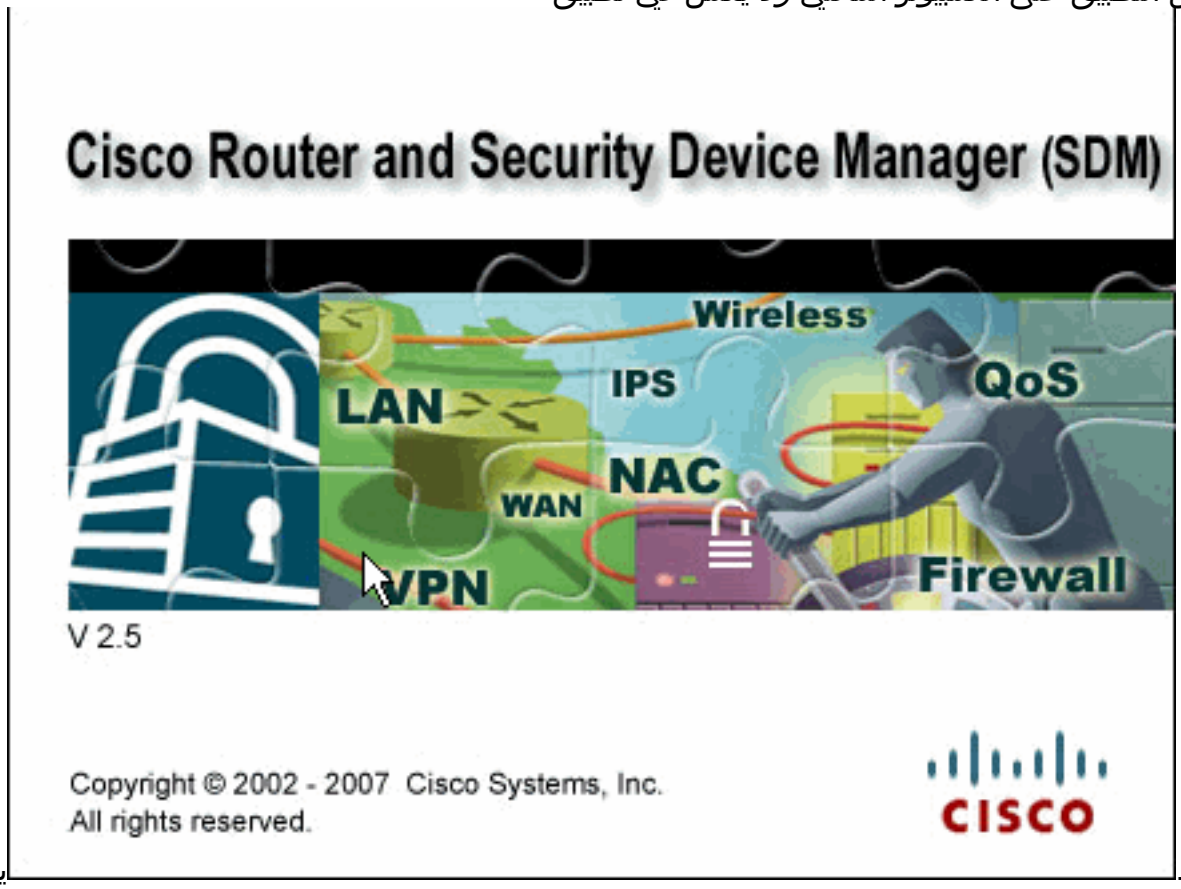
أتمت هذا steps in order to شكلت يقيد ال P2P حركة مرور على cisco ios مسحاج تخديد:

ملاحظة: لتكوين NBAR لاكتشاف حركة مرور البيانات لجميع البروتوكولات المعروفة ل NBAR على واجهة معينة، يجب إستخدام الأمر ip nbar protocol-discovery في وضع تكوين الواجهة أو وضع تكوين شبكة VLAN لتمكين

اكتشاف حركة مرور البيانات. قم بمتابعة تكوين إدارة قاعدة بيانات المحول (SDM) بعد تكوين اكتشاف البروتوكول على الواجهة المطلوبة حيث يتم إستخدام سياسة جودة الخدمة التي تم تكوينها.

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

1. افتح مستعرض، وأدخل عنوان IP الخاص بالموجه الذي تم تكوينه للوصول إلى إدارة قاعدة بيانات المحول (SDM). على سبيل المثال، https://<*SDM_Router_IP_ADDRESS*>تأكد من تخويل أية تحذيرات يعطيك المستعرض لها علاقة بموثوقية شهادة SSL. يكون كل من اسم المستخدم وكلمة المرور الافتراضيين فارغين.يعرض الموجه هذه النافذة للسماح بتنزيل تطبيق إدارة قاعدة بيانات المحول (SDM). يقوم هذا المثال بتحميل التطبيق على الكمبيوتر المحلي ولا يعمل في تطبيق

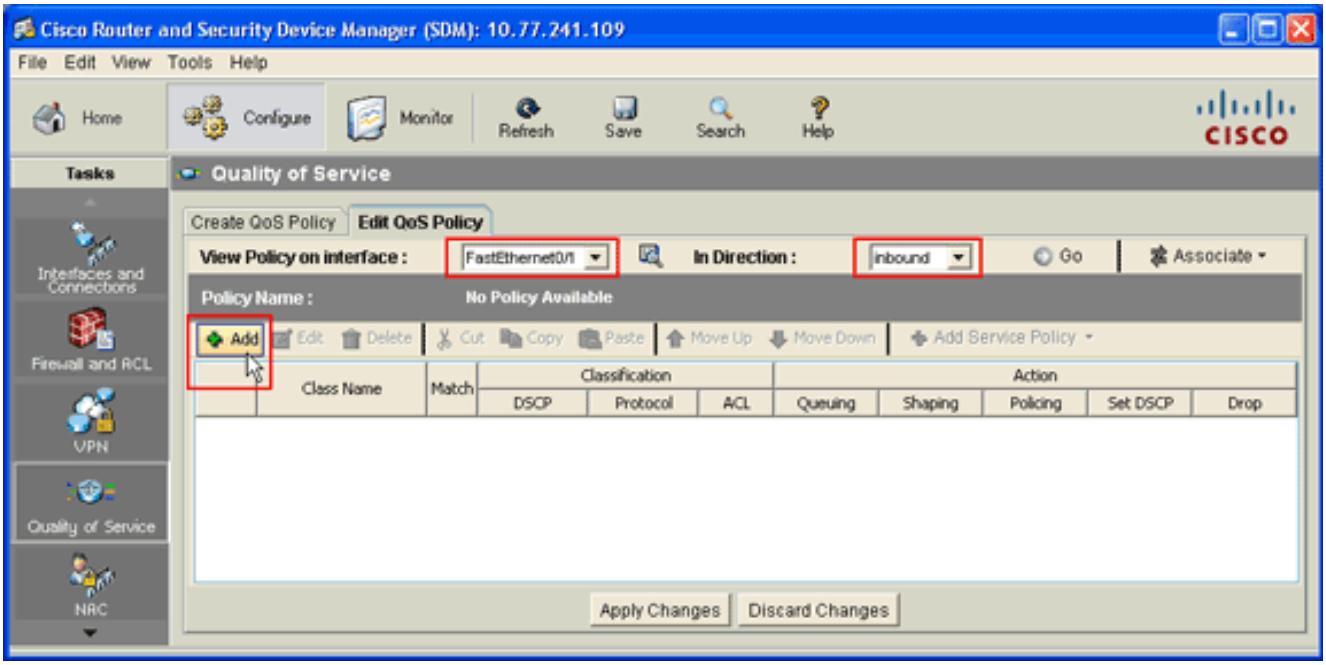


Java.يبدأ تنزيل إدارة قاعدة بيانات المحول (SDM) الآن.

2. بمجرد تنزيل مشغل إدارة قاعدة بيانات المحول (SDM)، قم بإكمال الخطوات التي توجهها المطالبات لتثبيت البرنامج وتشغيل مشغل إدارة قاعدة بيانات المحول (SDM) من Cisco.
3. أدخل اسم مستخدم وكلمة مرور، إذا قمت بتحديد واحد، ثم انقر على **موافق**.يستخدم هذا المثال **Cisco123** لاسم المستخدم و**Cisco123** ككلمة

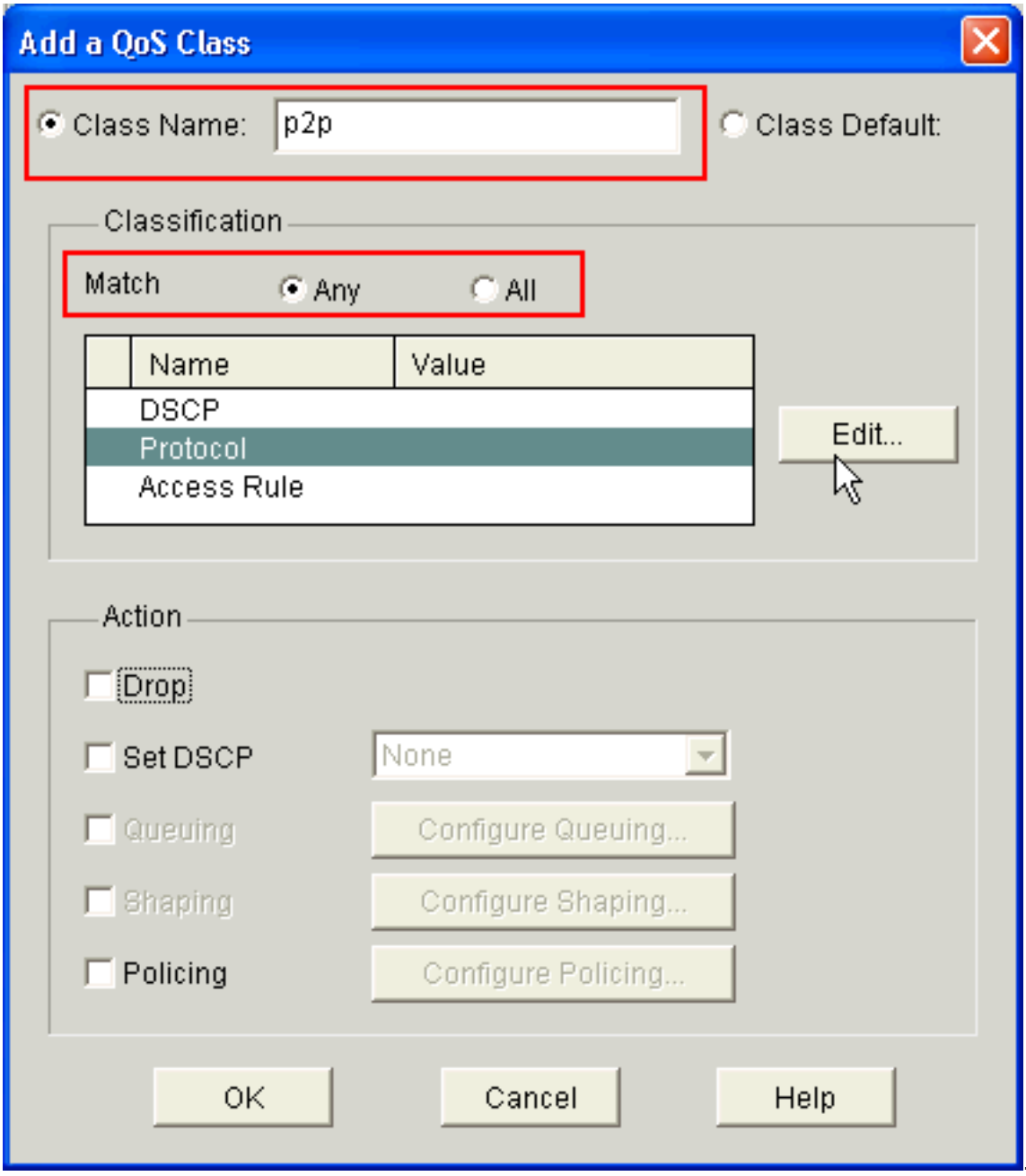
المرور.

4. أختر **تكوين > جودة الخدمة**، وانقر فوق علامة التبويب **Edit QoS Policy** (تحرير سياسة جودة الخدمة) في الصفحة الرئيسية ل SDM.



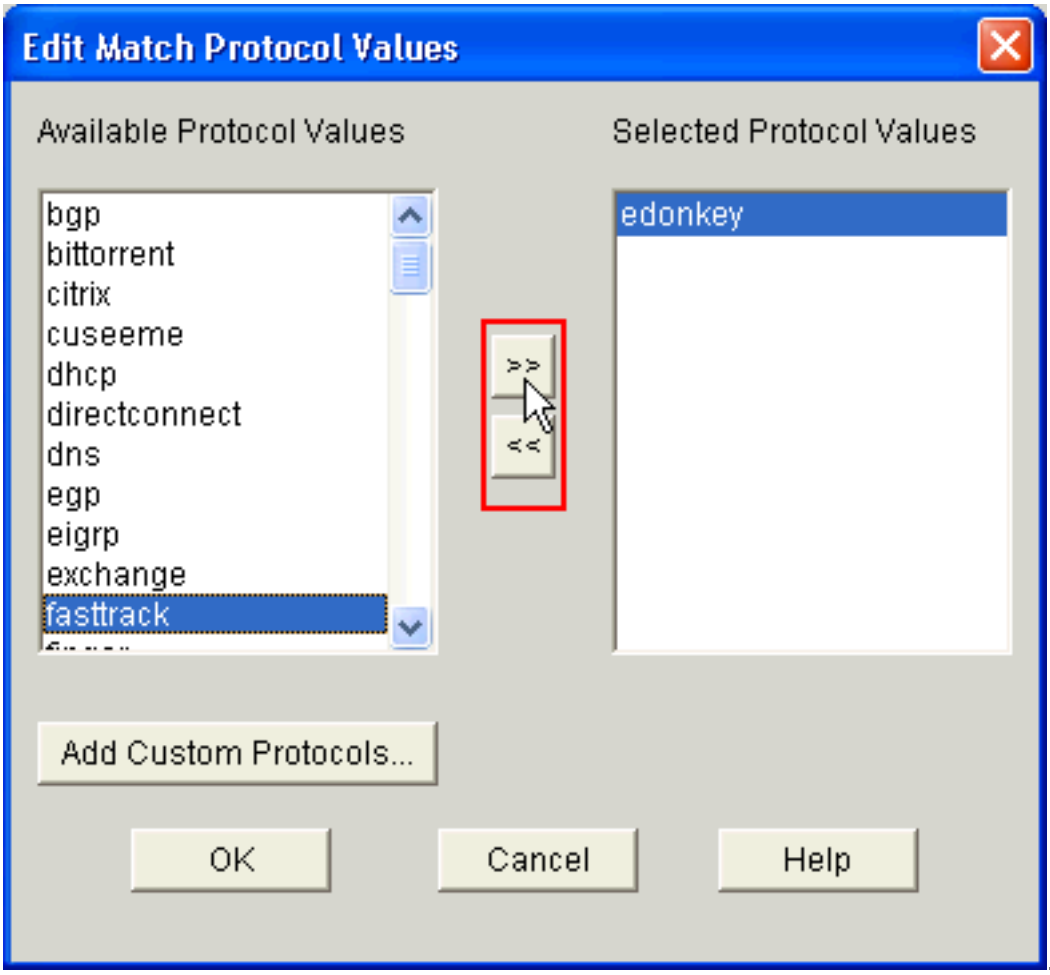
5. من القائمة المنسدلة "عرض النهج على الواجهة"، أختر اسم الواجهة، ثم أختر إتجاه تدفق حركة المرور (الوارد أو الصادر) من القائمة المنسدلة "في الإتجاه".في هذا المثال، تكون الواجهة *FastEthernet 0/1*، والاتجاه *الوارد*.

6. طقطقة **يضيف** in order to أضفت جديد qoS صنف للقارن.سوف يظهر مربع الحوار إضافة فئة جودة



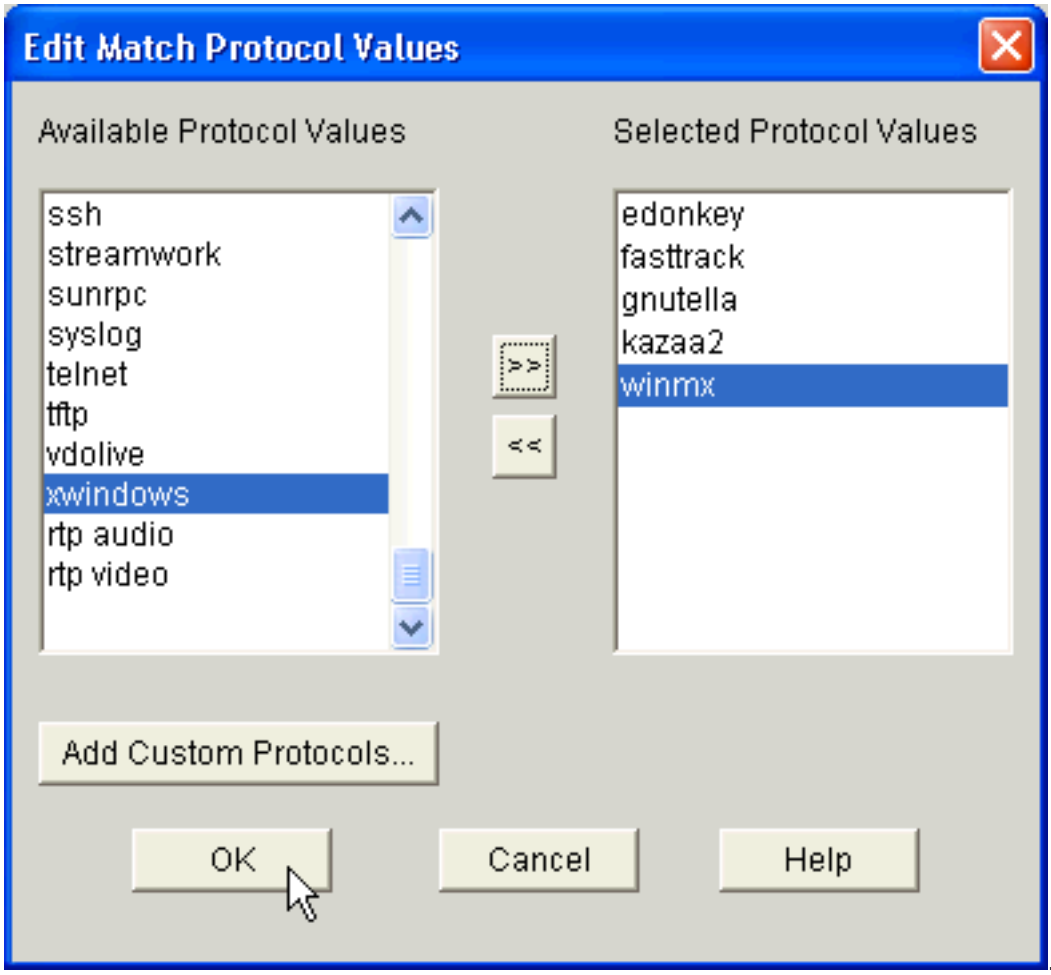
الخدمة.

7. إذا كنت ترغب في إنشاء فئة جديدة، انقر فوق زر الخيار **اسم الفئة**، وقم بإدخال اسم للفئة الخاصة بك. وإلا، انقر زر الخيار **الافتراضي للفئة** إذا كنت تريد إستخدام الفئة الافتراضية.يقوم هذا المثال بإنشاء فئة جديدة باسم *p2p*.
8. في منطقة التصنيف، انقر إما زر **أي** راديو أو **كل** الراديو لخيار التطابق.يستخدم هذا الأمثلة خيار *أي* تطابق، والذي يشغل الأمر class-map match-any p على الموجه.
9. حدد **بروتوكول** في قائمة التصنيف، وانقر فوق **تحرير** لتحرير معلمة البروتوكول.يظهر مربع الحوار تحرير قيم

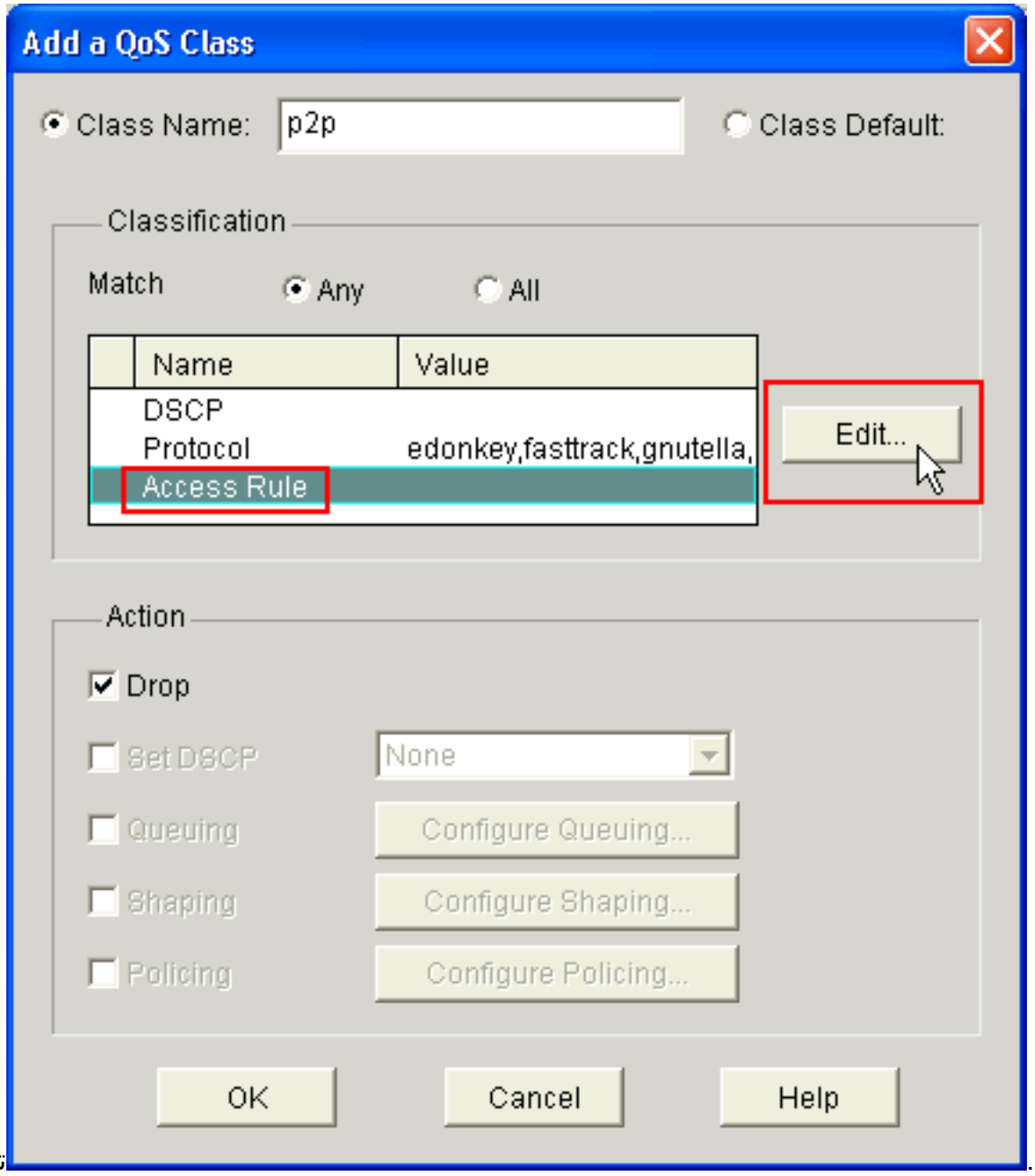


البروتوكول المطابقة.

10. من قائمة قيم البروتوكول المتاحة، حدد كل بروتوكول P2P تريد حظره، وانقر زر السهم الأيمن (>) لنقل كل بروتوكول إلى قائمة قيم البروتوكول المحددة.**ملاحظة:** لتصنيف حركة مرور P2P باستخدام NBAR، انتقل إلى صفحة تنزيل البرامج، وقم بتنزيل أحدث برنامج لوحدة اللغة لوصف بروتوكول (PDLM) P2P) وملفات القراءة. P2P PDLMs المتوفرة للتنزيل تشمل WinMx و BitBurst و Kazaa2 و Gnutella و eDonkey و FastTrack و Napster. وفقا لبرنامج IOS، قد لا تحتاج إلى أحدث إصدارات PDLM نظرا لأنه قد يتم دمج بعضها في برنامج IOS (على سبيل المثال، FastTrack وبرنامج Napster). وبمجرد تنزيلها، انسخ PDLMs إلى ذاكرة Flash (الذاكرة المؤقتة) الخاصة بالموجه، وقم بتحميلها إلى IOS من خلال تكوين **ip nbar pdlm *<flash_device>*:*<filename>*.pdlm**. قم بإصدار الأمر **show ip nbar pdlm** لضمان تحميله بنجاح. وبمجرد تحميلها، يمكنك إستخدامها في عبارات بروتوكول المطابقة ضمن تكوين خريطة الفئة.

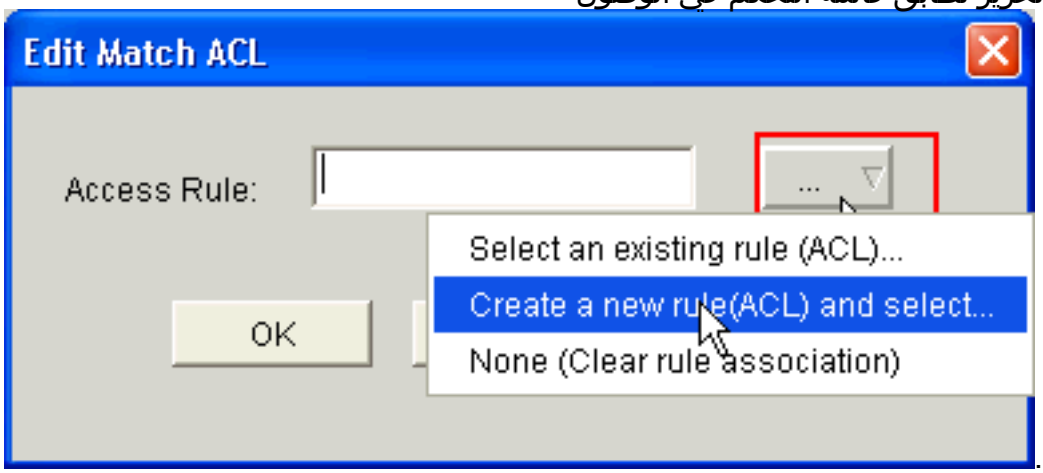


11. وانقر فوق **OK**.
12. في شاشة إضافة فئة جودة الخدمة، حدد **قواعد الوصول** من قائمة التصنيف، وانقر **تحرير** لإنشاء قاعدة وصول جديدة. يمكنك أيضا تعيين قاعدة وصول موجودة إلى خريطة فئة



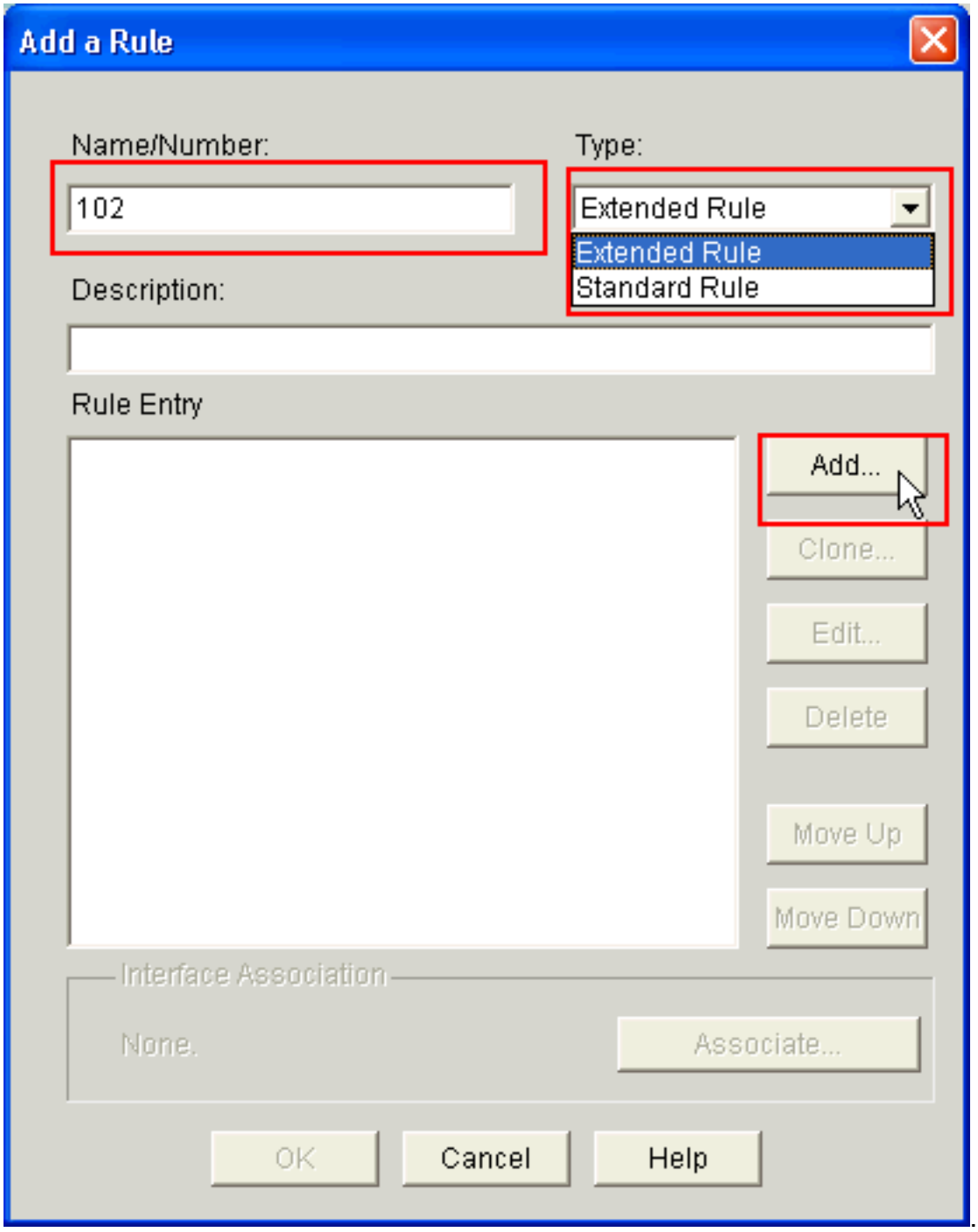
تظهر **p2p**.

شاشة تحرير تطابق قائمة التحكم في الوصول



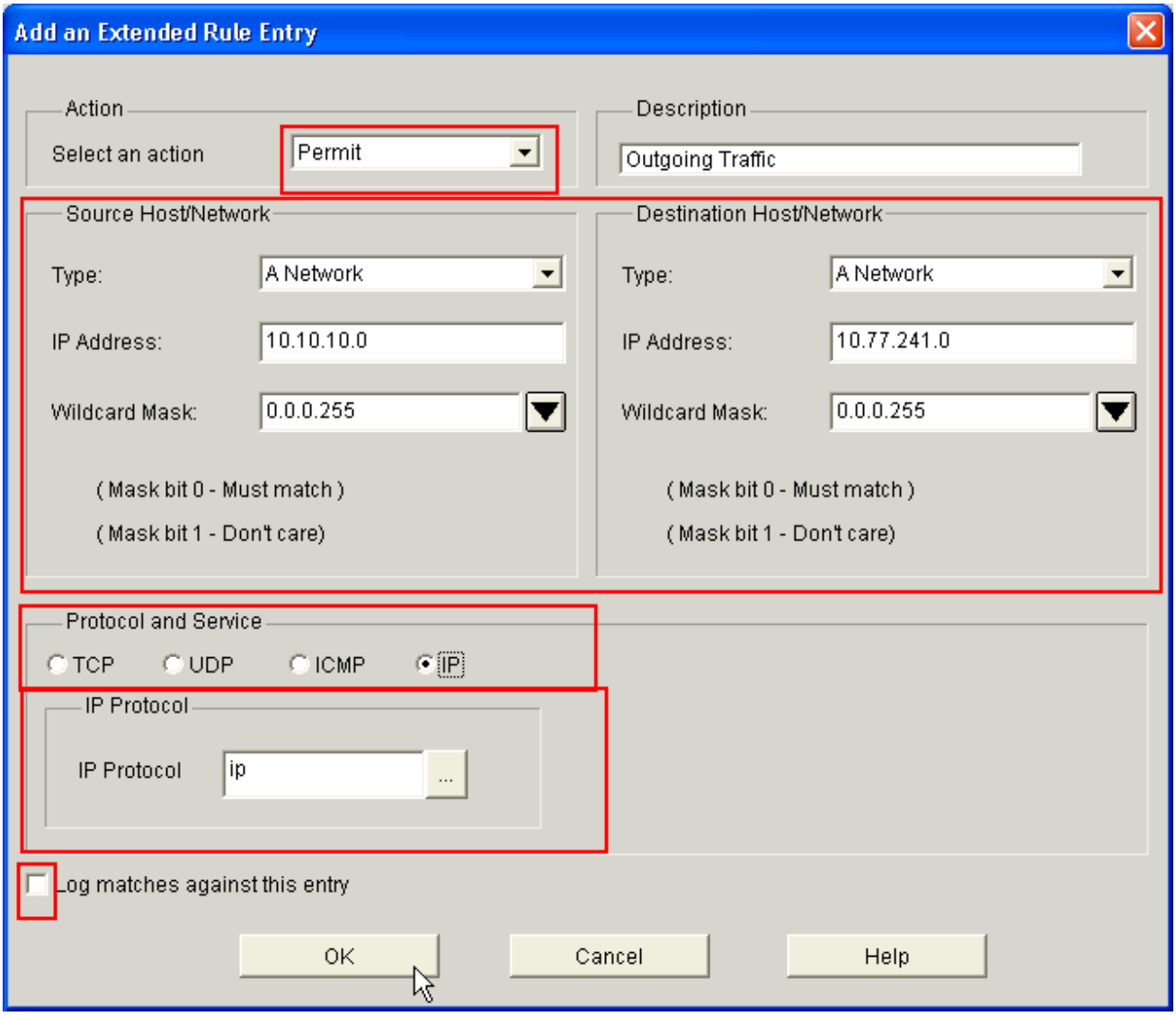
(ACL).

13. انقر زر قاعدة الوصول (...)، واختر الخيار المناسب. يقوم هذا المثال بإنشاء قائمة تحكم في الوصول (ACL) جديدة.يظهر مربع الحوار إضافة

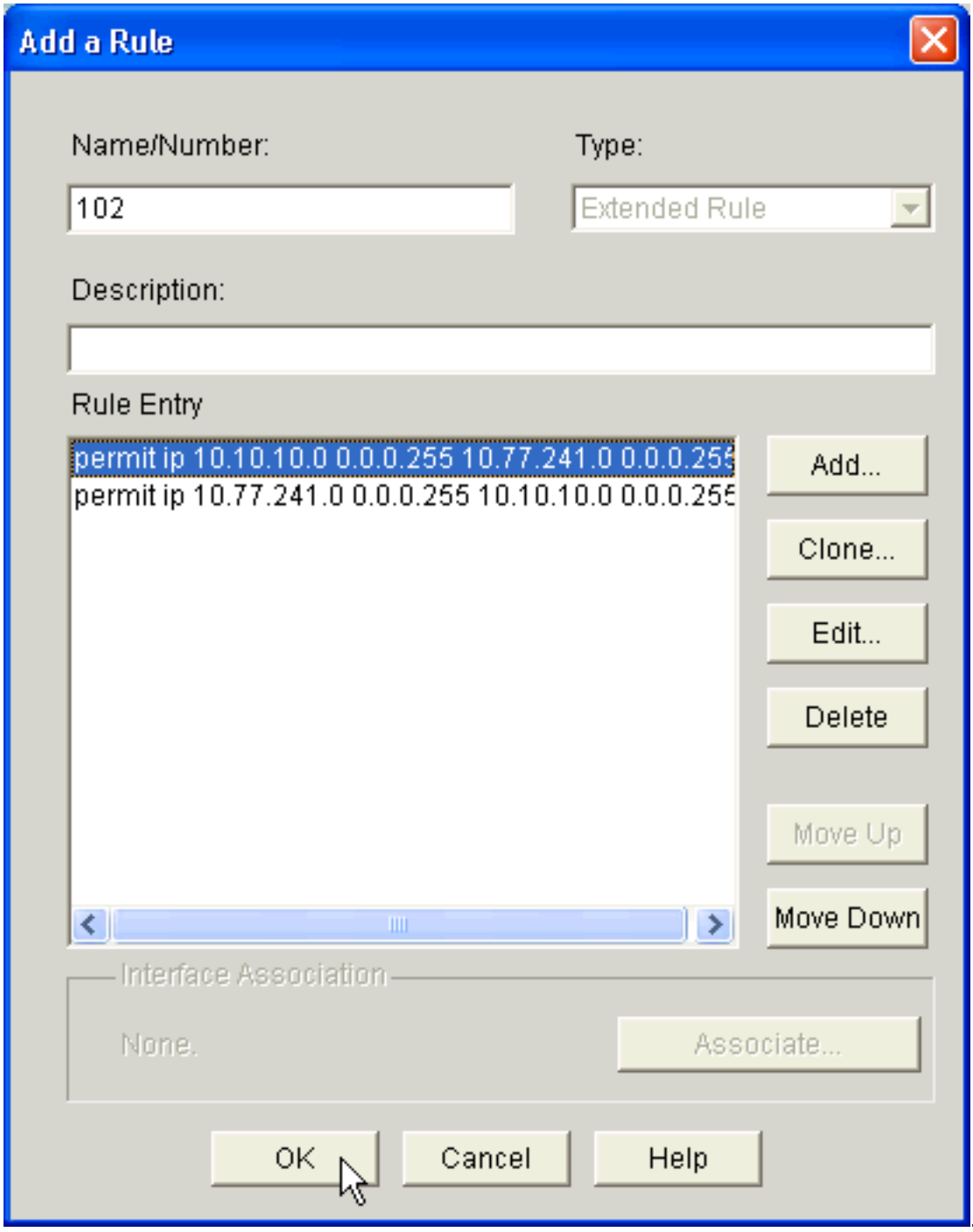


قاعدة.

14. في شاشة إضافة قاعدة، أدخل اسم أو رقم قائمة التحكم في الوصول (ACL) المطلوب إنشاؤه في حقل الاسم/الرقم لقائمة التحكم في الوصول (ACL).
15. من القائمة المنسدلة نوع ، أختر نوع قائمة التحكم في الوصول (ACL) التي سيتم إنشاؤها (إما *القاعدة الموسعة* أو *القاعدة القياسية*).
16. انقر فوق **إضافة** لإضافة تفاصيل إلى قائمة التحكم في الوصول (*102* ACL).تظهر شاشة إضافة إدخال قاعدة موسعة.

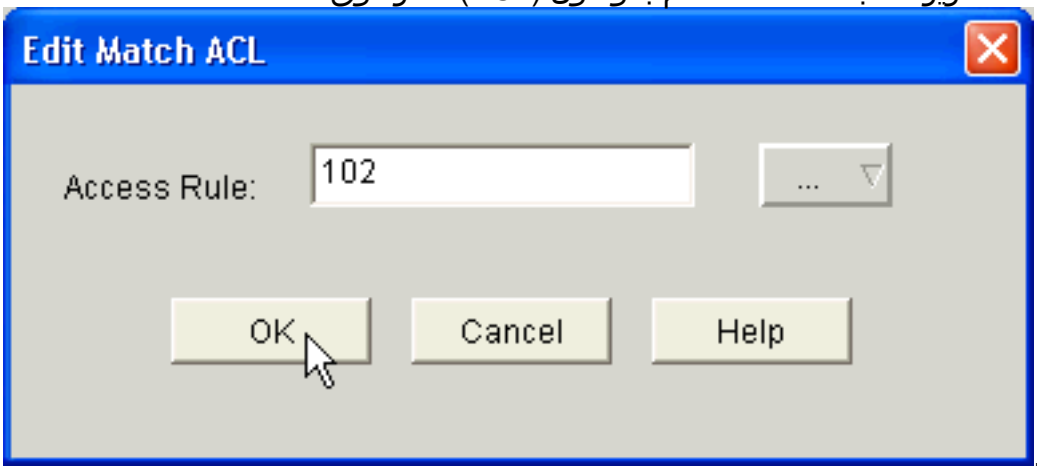


17. في شاشة إضافة إدخال قاعدة موسعة، أختر إجراء (إما *السماح* أو *الرفض*) من القائمة المنسدلة تحديد إجراء التي تشير إلى ما إذا كان يجب أن تسمح قاعدة قائمة التحكم في الوصول بحركة المرور بين شبكات المصدر والوجهة أو رفضها. هذه القاعدة لحركة المرور الصادرة من الشبكة الداخلية إلى الشبكة الخارجية.
18. دخلت معلومة للمصدر والغاية شبكة في المصدر مضيف/شبكة وغاية مضيف/شبكة منطقة على التوالي.
19. في منطقة "البروتوكول والخدمات"، انقر فوق زر الاختيار المناسب. يستخدم هذا المثال IP.
20. إذا كنت ترغب في تسجيل الحزم المطابقة مقابل قاعدة قائمة التحكم في الوصول هذه، فتحقق من **تطابقات السجل مقابل** خانة الاختيار **هذه الإدخال**.
21. وانقر فوق **OK**.
22. في شاشة إضافة قاعدة، انقر



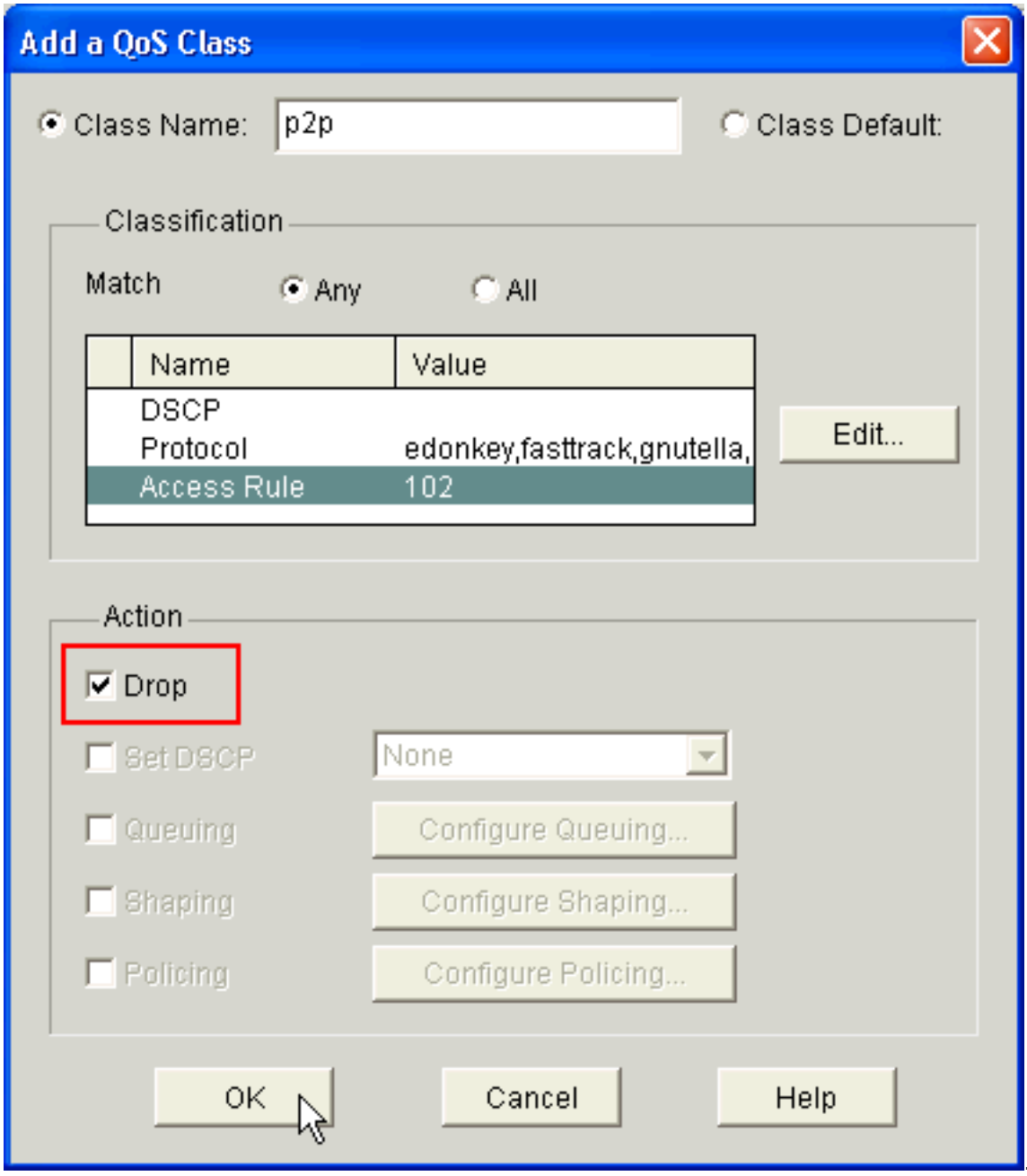
موافق.

23. في شاشة تحرير مطابقة قائمة التحكم بالوصول (ACL)، انقر فوق



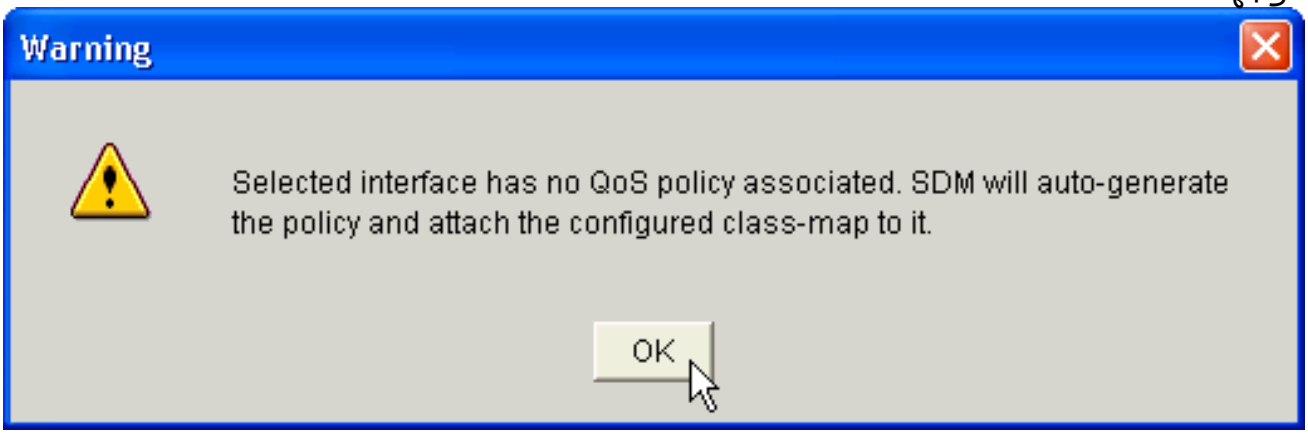
موافق.

24. في شاشة إضافة فئة جودة الخدمة، حدد خانة الاختيار **إسقاط** لإجبار الموجه على حظر حركة مرور



.P2P

25. وانقر فوق **OK**.يتم عرض رسالة التحذير التالية بشكل افتراضي حيث لم يتم تعيين سياسة جودة الخدمة إلى الواجهة.

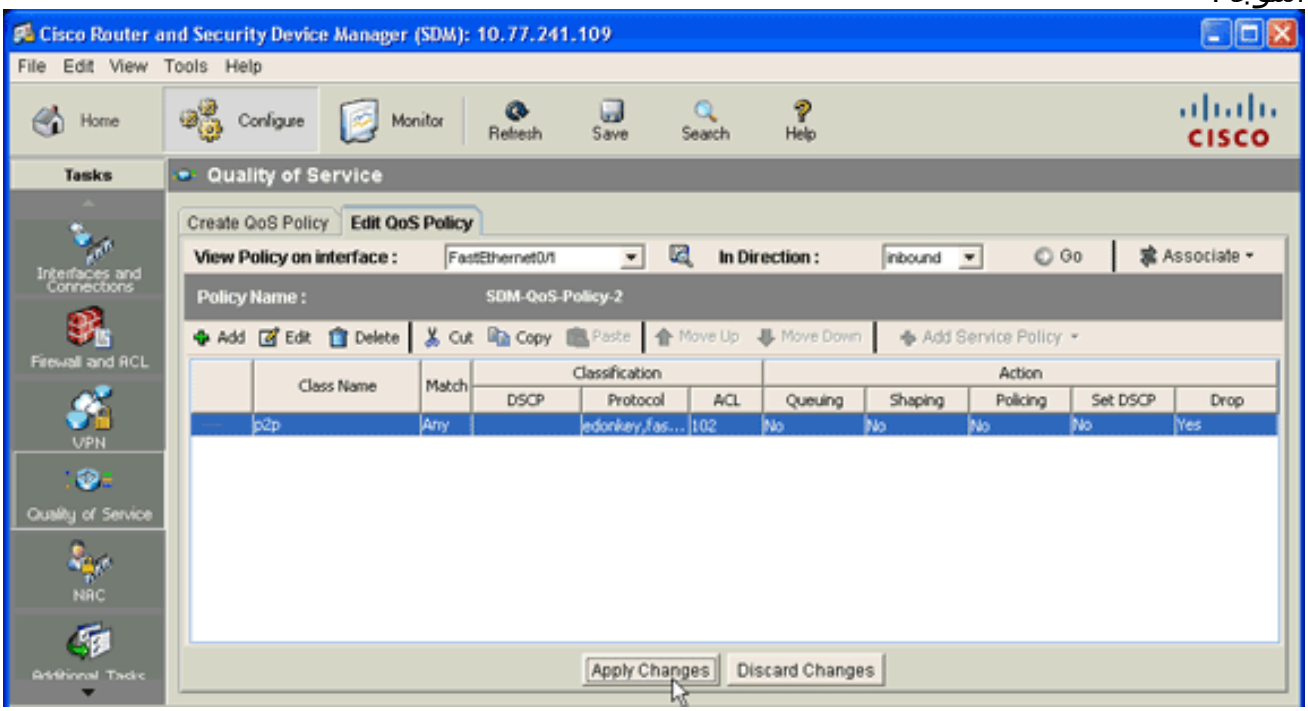


سيقوم إدارة قاعدة بيانات المحول (SDM) بإنشاء سياسة جودة الخدمة تلقائيا وإرفاق خريطة الفئة التي تم تكوينها بالسياسة. واجهة سطر الأوامر (CLI) المكافئة لخطوة تكوين SDM هذه هي:

```
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. في علامة التبويب "سياسة تحرير جودة الخدمة"، انقر فوق **تطبيق التغييرات** لتسليم التكوين إلى الموجه.



جدار حماية التطبيق — ميزة "تنفيذ حركة مرور الرسائل الفورية" في الإصدار T(4)12.4 من Cisco IOS والإصدارات الأحدث

فرض حركة مرور الرسائل الفورية

جدار حماية التطبيق—تتيح ميزة "فرض حركة مرور الرسائل الفورية" للمستخدمين إمكانية تحديد نهج يحدد أنواع حركة مرور الرسائل الفورية المسموح بها في الشبكة وفرض هذا النهج. يمكنك التحكم في عدة مراسلات (مثل AOL و Yahoo و MSN) في نفس الوقت عند تكوينها في **نهج APPFW** تحت **المراسلة الفورية للتطبيق**. لذلك، يمكن أيضا فرض الوظيفة الإضافية التالية:

- تكوين قواعد فحص الجدار الناري
- فحص الحزمة العميقة للحمولة (للبحث عن خدمات مثل المحادثة النصية)

ملاحظة: ميزة "تنفيذ حركة مرور الرسائل الفورية وجدار الحماية الخاص بالتطبيق" مدعومة في الإصدار T(4)12.4 من Cisco IOS والإصدارات الأحدث.

نهج تطبيق Instant Messenger

يستخدم جدار حماية التطبيق سياسة تطبيق، تتكون من مجموعة من التوقيعات الثابتة، لاكتشاف انتهاكات الأمان. التوقيع الثابت عبارة عن مجموعة من المعلمات تحدد شروط البروتوكول التي يجب استيفاؤها قبل إتخاذ الإجراء. يتم تحديد شروط البروتوكول وردود الفعل هذه من قبل المستخدم النهائي عبر واجهة سطر الأوامر لتكوين سياسة تطبيق.

تم تحسين جدار حماية تطبيق Cisco IOS لدعم سياسات تطبيق Messenger الأصلي الفوري. وبالتالي، يمكن لجدار حماية Cisco IOS الآن اكتشاف إتصالات المستخدم بخوادم Messenger الفورية (AIM) ل AOL و Yahoo ومنع هذه الاتصالات! خدمات المراسلة الفورية ل Messenger و MSN Messenger. تتحكم هذه الوظيفة في جميع الاتصالات للخدمات المدعومة، بما في ذلك إمكانيات النص والصوت والفيديو ونقل الملفات. يمكن رفض الطلبات الثلاثة أو السماح بها بشكل فردي. يمكن التحكم في كل خدمة بشكل فردي للسماح بخدمة دردشة النص، كما يتم تقييد خدمات الصوت ونقل الملفات والفيديو وغيرها من الخدمات. تزيد هذه الوظيفة من قدرة فحص التطبيق الموجودة للتحكم في حركة مرور تطبيق المراسلة الفورية (IM) التي تم تخزينها على هيئة حركة مرور HTTP (الويب). ارجع إلى

جدار حماية التطبيق - تطبيق حركة مرور الرسائل الفورية للحصول على مزيد من المعلومات.

ملاحظة: في حالة حظر تطبيق المراسلة الفورية، تتم إعادة تعيين الاتصال ويتم إنشاء رسالة syslog، حسب الاقتضاء.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر show. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

- **show ip nbar pdlm** — لعرض PDLM قيد الاستخدام بواسطة NBAR، أستخدم الأمر **show ip nbar pdlm** في وضع EXEC ذي الامتيازات:

```
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** — لعرض معلومات حول إصدار برنامج NBAR في إصدار Cisco IOS أو إصدار PDLM ل NBAR على موجه Cisco IOS الخاص بك، أستخدم الأمر **show ip nbar version** في وضع EXEC ذي الامتيازات:

```
R1#show ip nbar version

     NBAR software version:  6

 base                  Mv: 2   1
 ftp                   Mv: 2   2
 http                  Mv: 9   3
 static                Mv: 6   4
 tftp                  Mv: 1   5
 exchange              Mv: 1   6
 vdolive               Mv: 1   7
 sqlnet                Mv: 1   8
 rcmd                  Mv: 1   9
 netshow               Mv: 1  10
 sunrpc                Mv: 2  11
 streamwork            Mv: 1  12
citrix                Mv: 10  13
 fasttrack             Mv: 2  14
 gnutella              Mv: 4  15
 kazaa2                Mv: 7  16
 custom-protocols      Mv: 1  17
 rtsp                  Mv: 4  18
 rtp                   Mv: 5  19
 mgcp                  Mv: 2  20
 skinny                Mv: 1  21
 h323                  Mv: 1  22
 sip                   Mv: 1  23
 rtcp                  Mv: 2  24
 edonkey               Mv: 5  25
 winmx                 Mv: 3  26
 bittorrent            Mv: 4  27
 directconnect         Mv: 2  28
 skype                 Mv: 1  29
```

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

- show policy-map interface — لعرض إحصائيات الحزمة لجميع الفئات التي تم تكوينها لجميع سياسات الخدمة إما على الواجهة المحددة أو الواجهة الفرعية أو على دائرة افتراضية دائمة معينة (PVC) على الواجهة، أستخدم الأمر show policy-map interface في وضع EXEC ذي الامتيازات:

```
R1#show policy-map interface fastEthernet 0/1
                                    FastEthernet0/1

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

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

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

- show running-config policy-map— لعرض جميع تكوينات خريطة السياسة بالإضافة إلى تكوين خريطة السياسة الافتراضية، أستخدم الأمر show running-config policy-map:

```
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— لعرض المعلومات حول تكوين خريطة الفئة، أستخدم الأمر show running-config class-map:

```
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
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

- **show access-list**— لعرض تكوين قائمة الوصول التي يتم تشغيلها على موجه Cisco IOS، أستخدم الأمر **show access-list**:

```
R1#show access-lists
Extended IP access list 102
permit ip 10.10.10.0 0.0.0.255 10.77.241.0 0.0.0.255 10
permit ip 10.77.241.0 0.0.0.255 10.10.10.0 0.0.0.255 20
```

معلومات ذات صلة

- دليل تكوين أمان Cisco IOS، الإصدار 12.4 support-
- التعرف على التطبيق المستند إلى الشبكة (NBAR)
- إعادة التوجيه السريع ((CEF Cisco Express Forwarding)
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).