تكوين مركز Cisco VPN 3000 للحجب باستخدام المرشحات وتعيين مرشح RADIUS

المحتويات

المقدمة

في نموذج التكوين هذا، نريد إستخدام عوامل التصفية للسماح للمستخدم بالوصول إلى خادم واحد فقط (10.1.1.2) داخل الشبكة ومنع الوصول إلى جميع الموارد الأخرى. يمكن إعداد مركز Cisco VPN 3000 للتحكم في بروتوكول IPsec، وبروتوكول الاتصال النفقي من نقطة إلى نقطة (PPTP)، ووصول عميل L2TP إلى موارد الشبكة باستخدام عوامل التصفية. تتكون عوامل التصفية من القواعد، والتي تكون مماثلة لقوائم الوصول على الموجه. إذا تم تكوين موجه ل:

```
access-list 101 permit ip any host 10.1.1.2
access-list 101 deny ip any any
```

سيكون مكافئ مركز الشبكة الخاصة الظاهرية (VPN) هو إعداد مرشح باستخدام القواعد.

القاعدة الأولى لتركيز الشبكة الخاصة الظاهرية (VPN) هي **allowed_server_rule**، والتي تعادل الأمر **allowed ip any host 10.1.1.2 الخاص** بالموجه. تتمثل قاعدة مركز الشبكة الخاصة الظاهرية (VPN) الثانية لدينا في **deny_server_rule** وهو ما يعادل أمر **deny ip any** للموجه.

إن عامل تصفية مركز VPN الخاص بنا هو **filter_with_2_rules**، وهو ما يعادل قائمة وصول الموجه 101، إنه يستخدم **allow_server_rule** و**deny_server_rule** (بهذا الترتيب). يفترض أنه يمكن للعملاء الاتصال بشكل صحيح قبل إضافة عوامل التصفية؛ فهم يتلقون عناوين IP الخاصة بهم من تجمع على مركز الشبكة الخاصة الظاهرية (VPN).

ارجع إلى PIX/ASA 7.x ASDM: تقييد الوصول إلى الشبكة الخاصة بمستخدمي VPN للوصول عن بعد لمعرفة المزيد حول السيناريو الذي يقوم فيه PIX/ASA 7.x بحظر الوصول من مستخدمي VPN.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

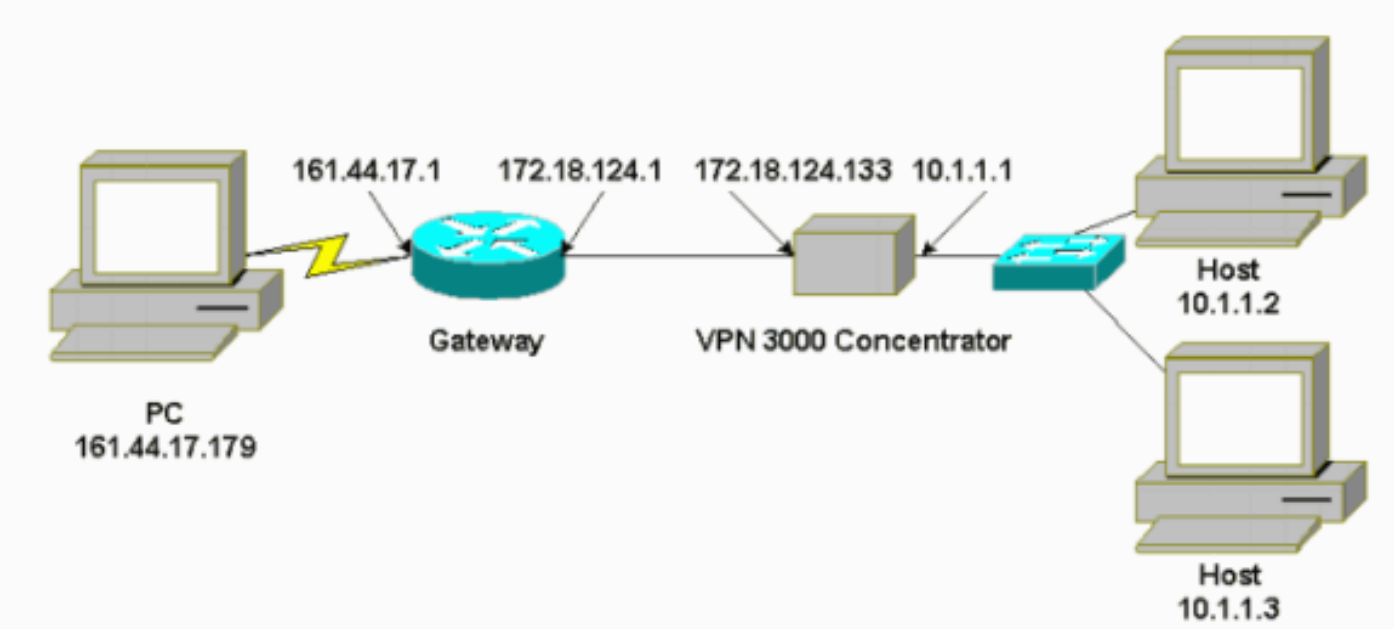
المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى الإصدار D.2.5.2 من Cisco VPN 3000 Concentrator.

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.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



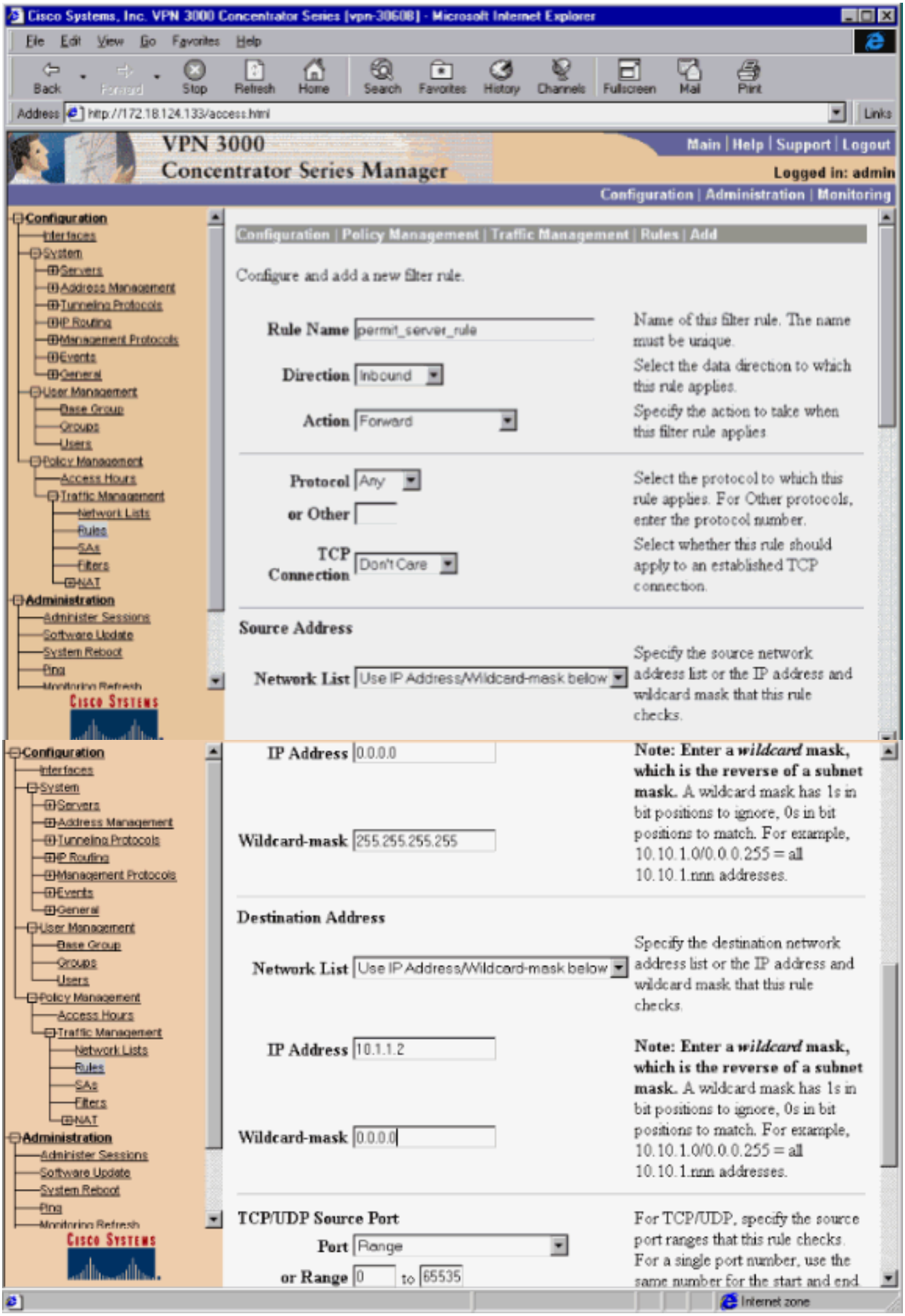
الاصطلاحات

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

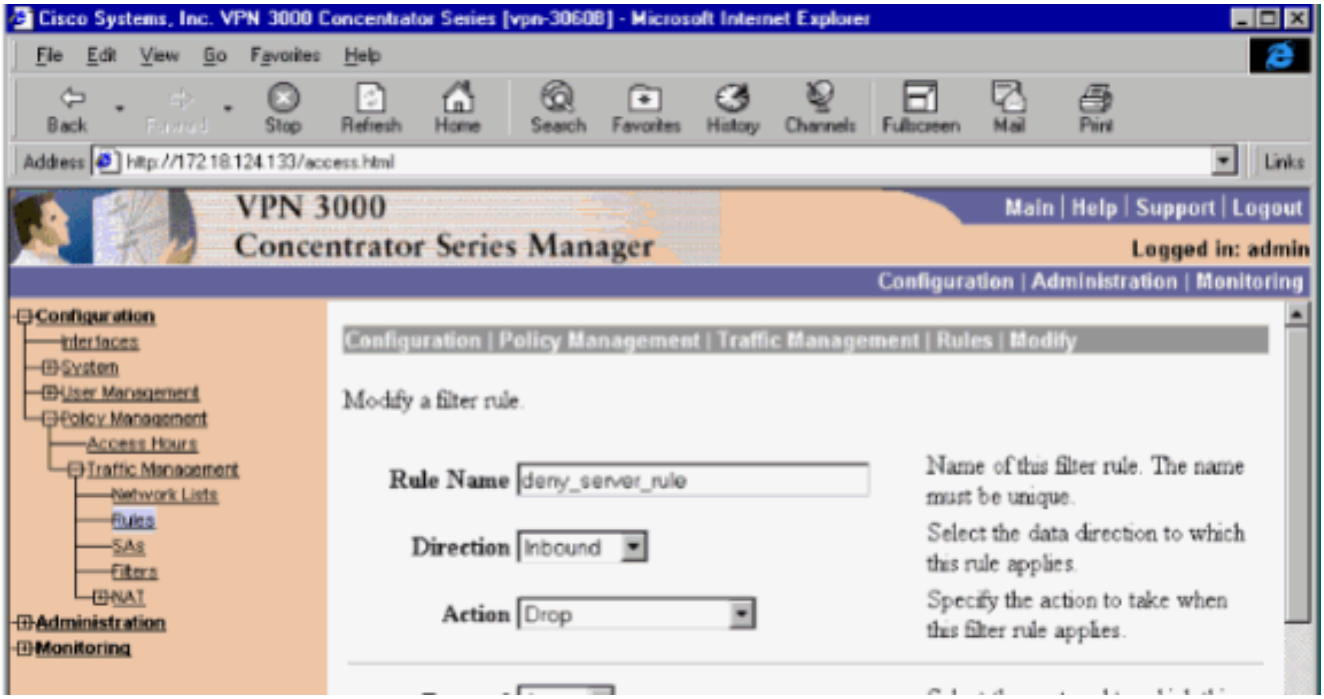
تكوين VPN 3000

أتمت هذا steps in order to شكلت ال VPN 3000 مركز.

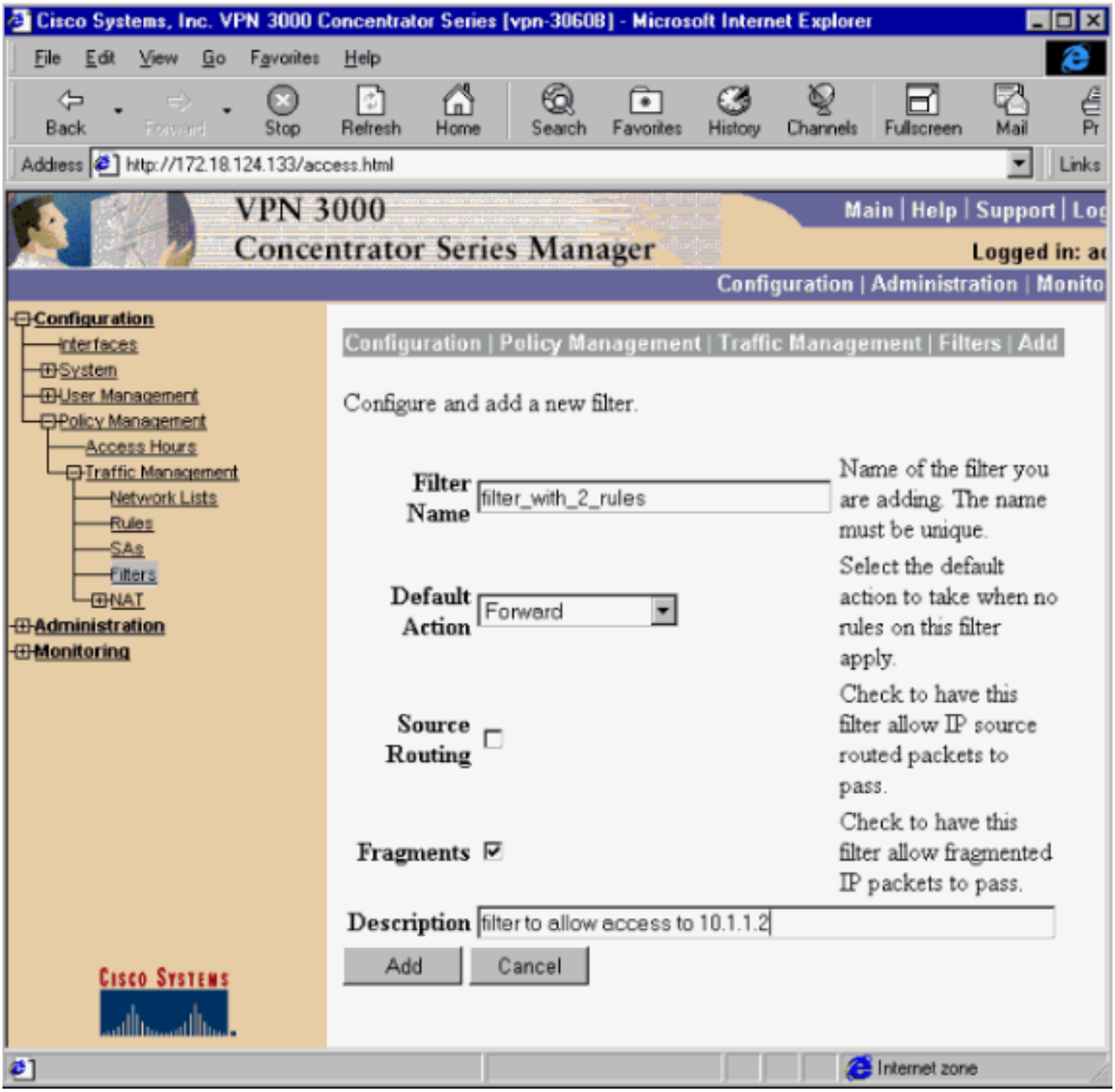
1. أخترت **تشكيل>إدارة سياسة>حركة مرور إدارة>قاعدة>إضافة** وتحديد أول قاعدة مركز VPN يدعو **enable_server_rule** مع هذه الإعدادات:الإتجاه - **الوارد**العمل — **إلى الأمام**عنوان المصدر - **255.255.255.255**عنوان الوجهة-**10.1.1.2**قناع حرف البدل-**0.0.0.0**



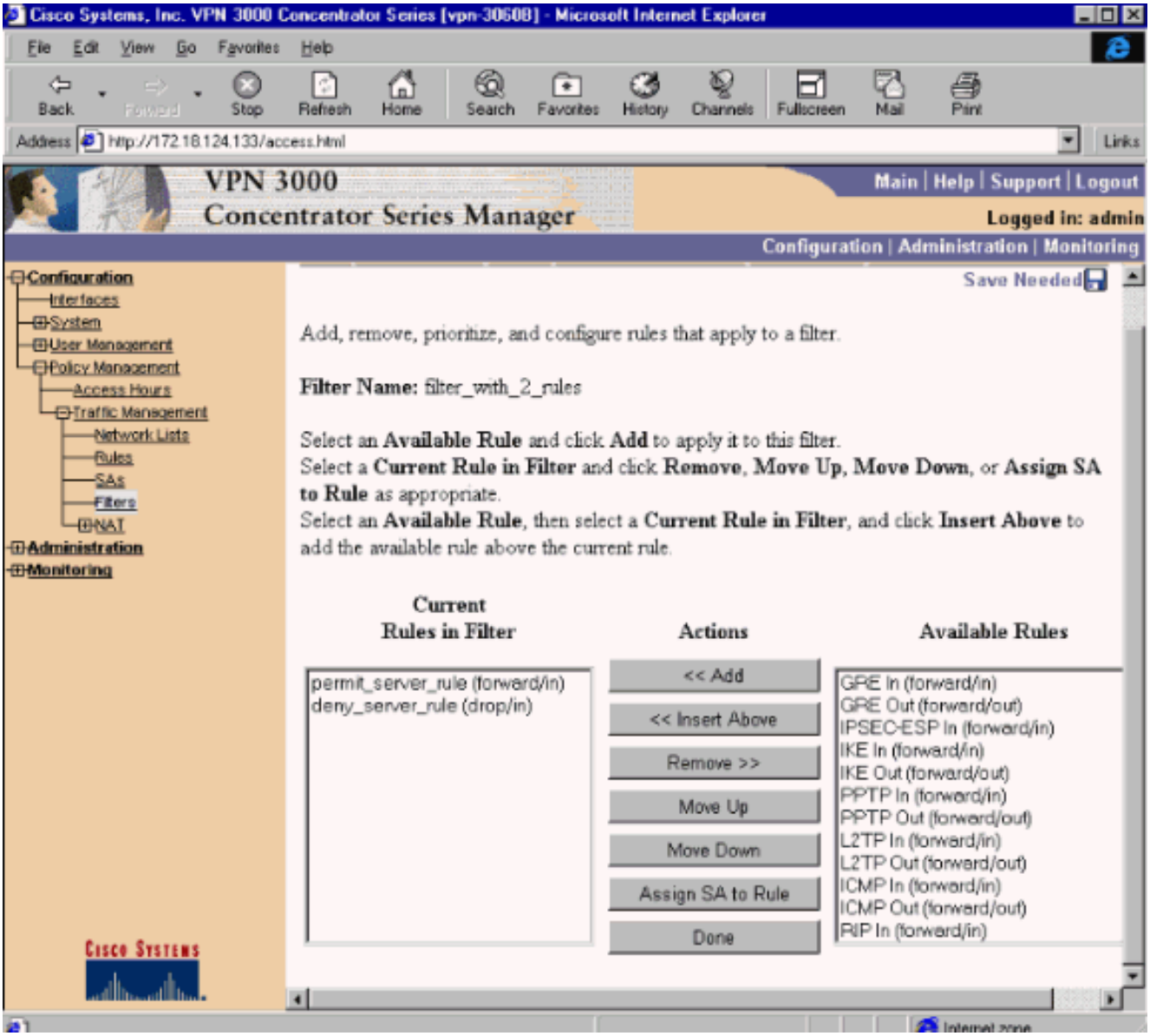
2. في نفس المنطقة، قم بتعريف القاعدة الثانية لتركيز شبكات VPN التي تسمى **deny_server_rule** باستخدام الإعدادات الافتراضية التالية:الإتجاه - **الوارد**الإجراء - **الإسقاط**عناوين المصدر والوجهة لأي شيء (255.255.255.255):



3. أختر **تكوين > إدارة السياسة > إدارة حركة مرور البيانات > عوامل التصفية** وأضف عامل تصفية **filter_with_2_rules** الخاص بك.



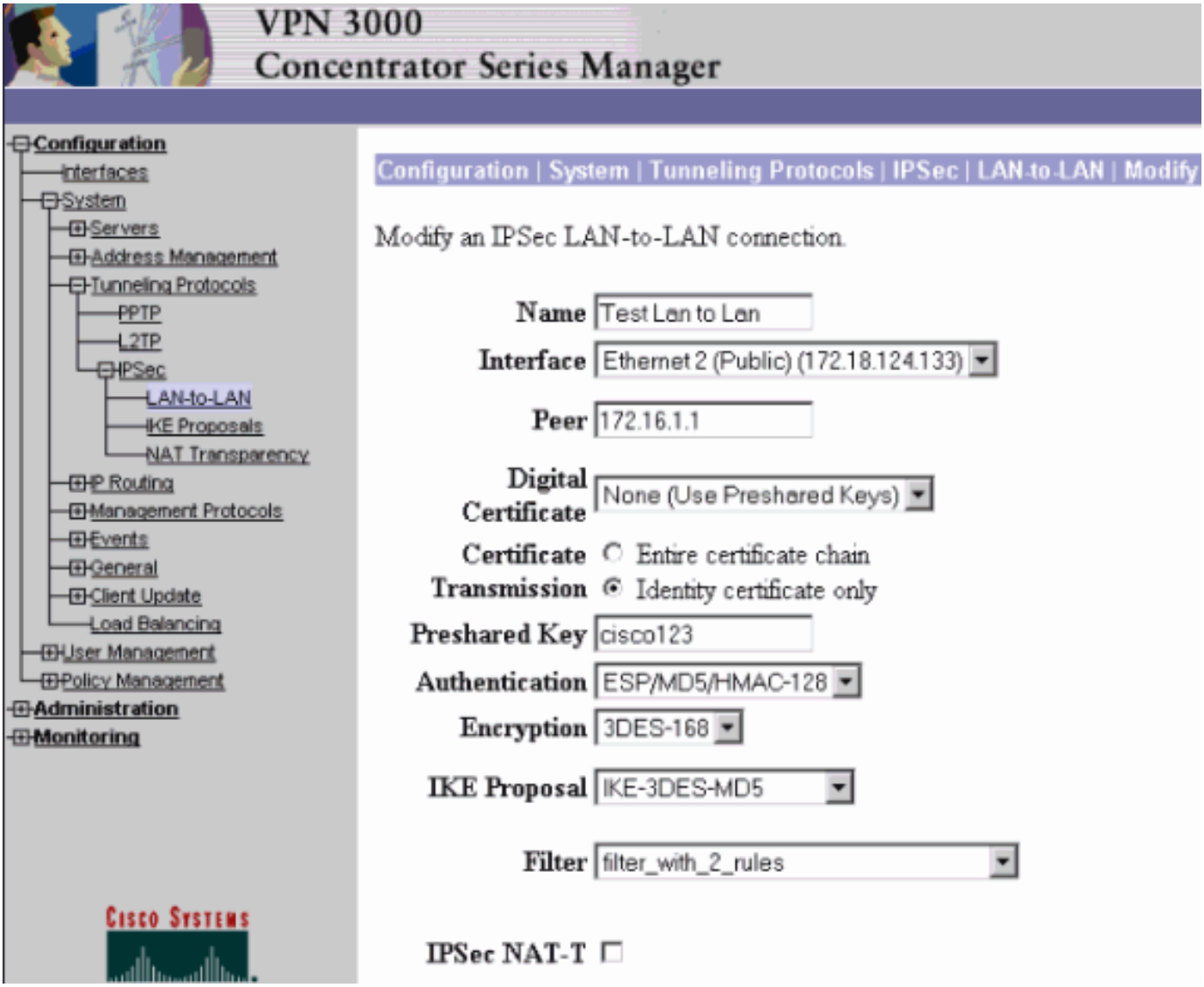
4. قم بإضافة القاعدتين ل filter_with_2_rules:



5. أختر **تكوين > إدارة المستخدم > مجموعات** وطبق المرشح على المجموعة:

عوامل تصفية نفق VPN من LAN إلى LAN

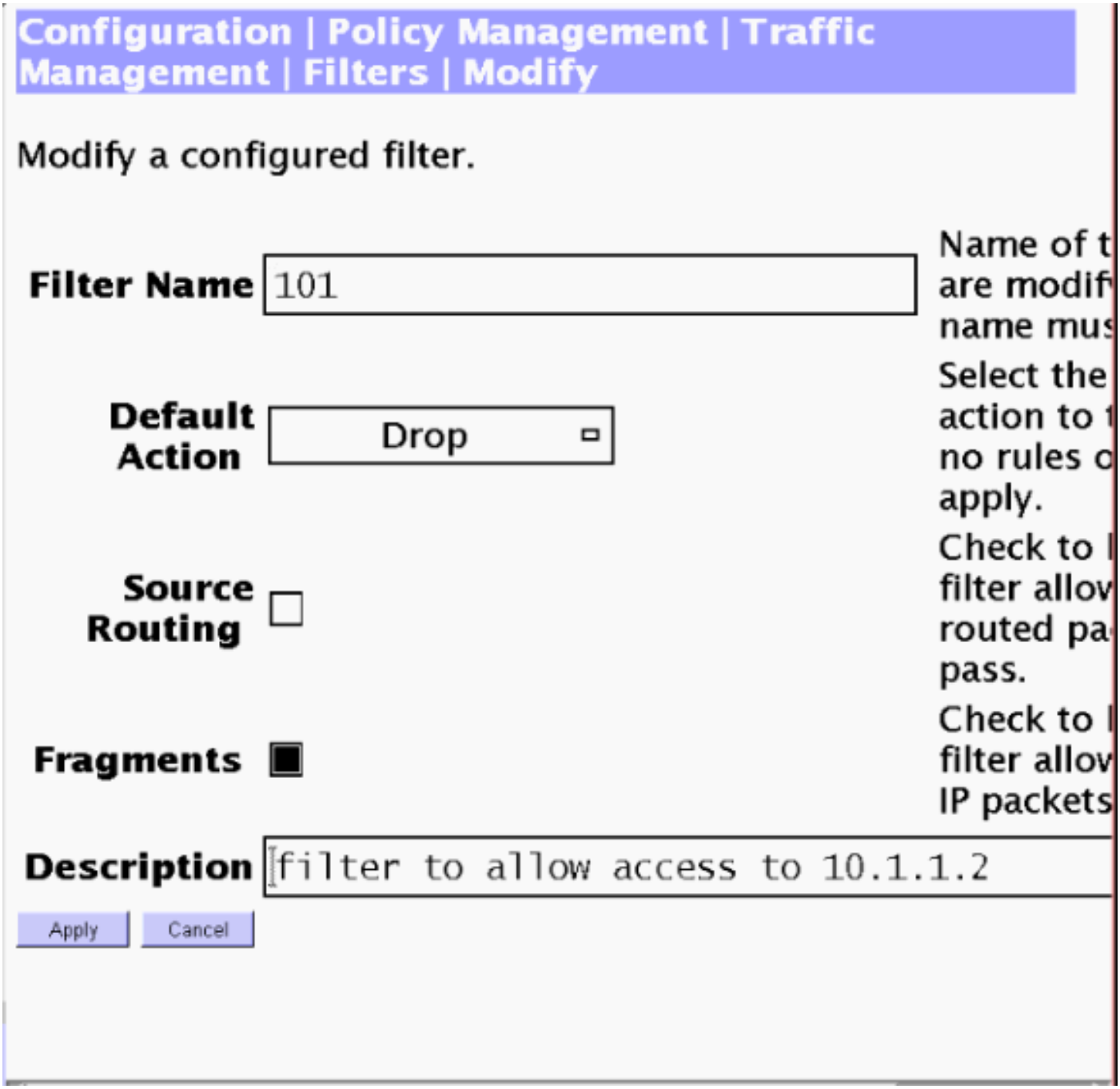
من رمز مركز VPN 3.6 والإصدارات الأحدث، يمكنك تصفية حركة مرور البيانات لكل نفق من شبكة LAN إلى شبكة IPsec لشبكة VPN. على سبيل المثال، إذا قمت بإنشاء نفق من شبكة LAN إلى مركز VPN آخر بعنوان 172.16.1.1، وتريد السماح للمضيف بوصول 10.1.1.2 إلى النفق أثناء رفض جميع حركات المرور الأخرى، فيمكنك تطبيق **filter_with_2_rules** عند إختيار **التكوين > النظام > بروتوكولات أنفاق > LAN < IPSec إلى شبكة VPN > تعديل** وتحديد **عامل التصفية_with_2_rules** تحت عاملالتصفية.



تكوين VPN 3000 - تعيين مرشح RADIUS

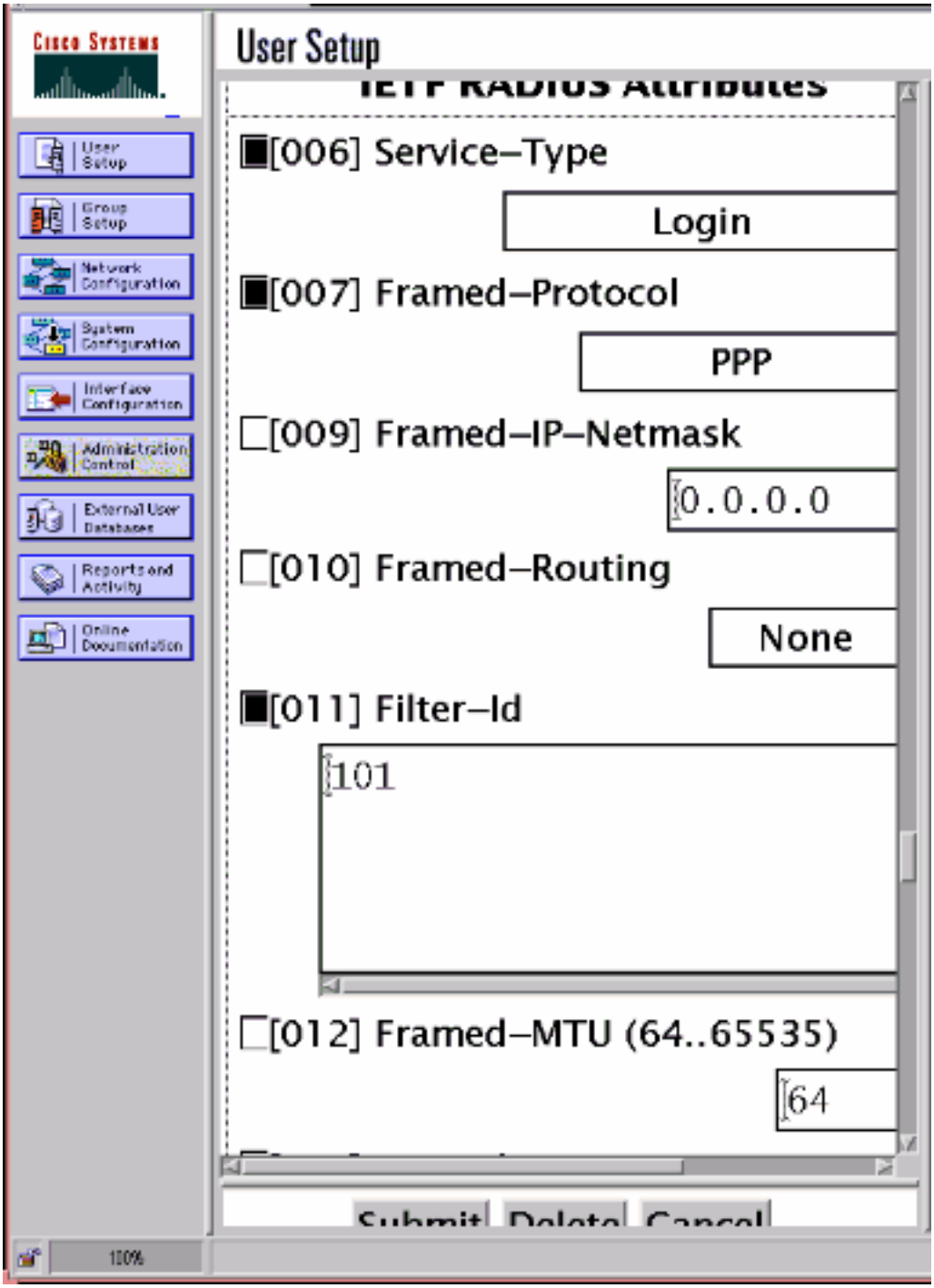
كما من الممكن تعريف عامل تصفية في مركز الشبكة الخاصة الظاهرية (VPN) ثم تمرير رقم عامل التصفية من خادم RADIUS (في شروط RADIUS، تكون السمة 11 هي معرف عامل التصفية)، حتى عندما تتم مصادقة المستخدم على خادم RADIUS، يكون معرف عامل التصفية مقترنا بذلك الاتصال. في هذا المثال، يفترض أن مصادقة RADIUS الخاصة بمستخدمي مركز VPN تكون قيد التشغيل بالفعل ولا يمكن إضافة إلا معرف التصفية.

قم بتعريف عامل التصفية على مركز VPN كما هو الحال في المثال السابق:



تكوين خادم CSNT - تعيين مرشح RADIUS

قم بتكوين السمة 11، Filter-id على خادم Cisco Secure NT لتكون **101**:



تصحيح الأخطاء - تعيين مرشح RADIUS

إذا كان AUTHDECODE (مستوى الخطورة 1-13) قيد التشغيل في مركز VPN، يظهر السجل أن خادم Cisco Secure NT يرسل أسفل قائمة الوصول 101 في السمة 11 (0x0b):

```
          SEV=13 AUTHDECODE/0 RPT=228 11:27:58.100 01/24/2001 207
020C002B 768825C5 C29E439F 4C8A727A     ...+v.%...C.L.rz :0000
..............EA7606C5 06060000 00020706 00000001     .v :0010
  ......0B053130 310806FF FFFFFF                   ..101 :0020
```

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

لأغراض أستكشاف الأخطاء وإصلاحها فقط، يمكنك تشغيل تصحيح أخطاء المرشح عند إختيار **التكوين > النظام > الأحداث > الفئات** وإضافة الفئة **Filterdbg** التي تكون درجة الخطورة **إلى السجل = 13**. في القواعد، قم بتغيير الإجراء الافتراضي من إعادة التوجيه (أو الإسقاط) إلى **إعادة التوجيه وتسجيل الدخول** (أو إسقاط وتسجيل). عند إسترداد سجل الأحداث في **المراقبة > سجل الأحداث**، يجب أن يعرض إدخالات مثل:

```
SEV=9 FILTERDBG/1 RPT=62 14:20:17.190 12/21/2000 221
Deny In: intf 1038, ICMP, Src 10.99.99.1, Dest 10.1.1.3, Type 8

SEV=9 FILTERDBG/1 RPT=63 14:20:18.690 12/21/2000 222
Deny In: intf 1038, ICMP, Src 10.99.99.1, Dest 10.1.1.3, Type 8
```

معلومات ذات صلة

- مفاوضة IPSec/بروتوكولات IKE
- الأسئلة المتداولة حول VPN 3000 Concentrator
- دعم RADIUS
- دعم مركز Cisco VPN 3000
- دعم عميل Cisco VPN 3000
- مصدر المحتوى الإضافي الآمن من Cisco لدعم Windows
- طلب التعليقات (RFCs)
- 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).