تكوين IPSec من عميل VPN 3.5 لمحادثة إلى مركز VPN 3000 على Solaris

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين عميل VPN 3.5 ل Solaris 2.6 للاتصال بموجه VPN 3000.

المتطلبات الأساسية

المتطلبات

قبل محاولة هذا التكوين، يرجى التأكد من استيفاء المتطلبات الأساسية التالية.

- يستخدم هذا المثال مفتاح مشترك مسبقا لمصادقة المجموعة. يتم التحقق من اسم المستخدم وكلمة المرور (المصادقة الموسعة) مقابل قاعدة البيانات الداخلية لمركز تركيز الشبكة الخاصة الظاهرية (VPN).
- يجب تثبيت عميل شبكة VPN بشكل صحيح. ارجع إلى تثبيت عميل VPN ل Solaris للحصول على تفاصيل حول التثبيت.
- يجب أن يكون اتصال IP موجودا بين عميل الشبكة الخاصة الظاهرية (VPN) والواجهة العامة لمركز تجميع الشبكة الخاصة الظاهرية (VPN). يجب تعيين قناع الشبكة الفرعية ومعلومات البوابة بشكل صحيح.

المكونات المستخدمة

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

- عميل Cisco VPN ل Solaris 2.6 الإصدار 3.5، صورة 3DES. (اسم الصورة: vpnclient-solaris5.6-3.5.rel-

(k9.tar.z

- نوع مركز VPN من Cisco: الإصدار Bootcode Rev: Altiga Networks/VPN Concentrator 3005 version 2.2.int_9 يناير 19 2000 05:36:41 Software Rev: Cisco Systems، Inc./VPN 3000 Concentrator Series، الإصدار rel August 06 20013:47:37.3.1

تم إنشاء المعلومات المُقدمة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كنت تعمل في شبكة مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر قبل استخدامه.

الاصطلاحات

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

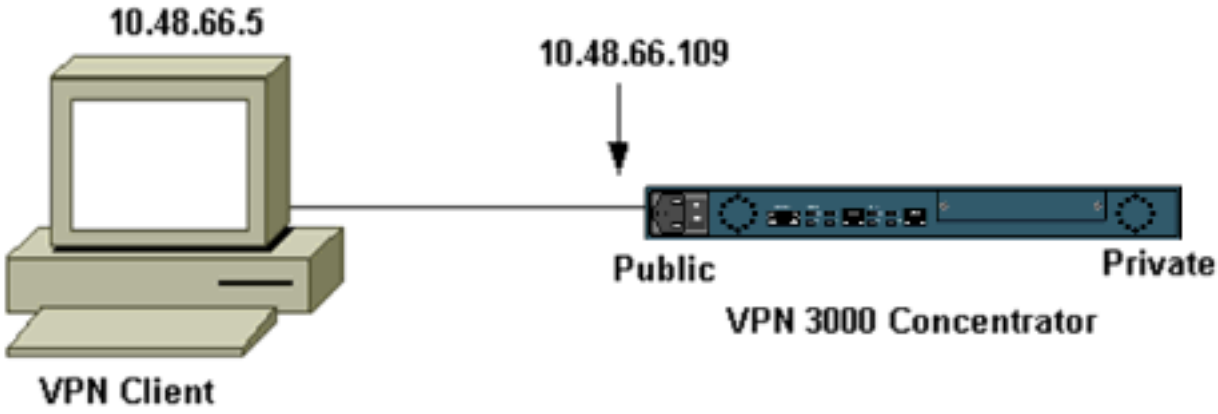
التكوين

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

ملاحظة: للعثور على معلومات إضافية حول الأوامر المستخدمة في هذا المستند، أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط).

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة الموضح في الرسم التخطيطي أدناه.



ملاحظة: لكي يتصل عميل الشبكة الخاصة الظاهرية (VPN) الإصدار 3.5 بمجمع الشبكة الخاصة الظاهرية (VPN)، يلزمك إصدار 3.0 أو إصدار أحدث على مركز الشبكة الخاصة الظاهرية (VPN).

التكوينات

إنشاء ملف تعريف مستخدم للاتصال

يتم تخزين ملفات تعريف المستخدم في دليل /etc/CiscoSystemsVPNClient/Profile. تحتوي هذه الملفات النصية على امتداد .pcf وتحتوي على المعاملات اللازمة لإنشاء اتصال بمركز VPN. يمكنك إنشاء ملف جديد أو تحرير ملف موجود. يجب أن تجد نموذج ملف تعريف، sample.pcf، في دليل ملف التعريف. يتبع هذا المثال إستخدام هذا الملف لإنشاء ملف تخصيص جديد باسم toCORPORATE.pcf.

```
/cholera]: ~ > cd /etc/CiscoSystemsVPNClient/Profiles]
cholera]: /etc/CiscoSystemsVPNClient/Profiles > cp sample.pcf toCORPORATE.pcf]
```

يمكنك إستخدام محرر النصوص المفضل لديك لتحرير هذا الملف الجديد إلى CORPORATE.pcf. قبل أي تعديل، يبدو الملف كما يلي.

ملاحظة: إذا كنت تريد إستخدام IPSec عبر ترجمة عنوان الشبكة (NAT)، فيجب أن يقول إدخال enableNat في التكوين أدناه "enableNat=1" بدلا من "enableNat=0".

```
[main]
Description=sample user profile
Host=10.7.44.1
AuthType=1
GroupName=monkeys
EnableISPConnect=0
ISPConnectType=0
=ISPConnect
=ISPCommand
Username=chimchim
SaveUserPassword=0
EnableBackup=0
=BackupServer
EnableNat=0
CertStore=0
=CertName
=CertPath
=CertSubjectName
CertSerialHash=00000000000000000000000000000000
DHGroup=2
ForceKeepAlives=0
```

ارجع إلى توصيفات المستخدم للحصول على وصف للكلمات الأساسية لملف تعريف المستخدم.

لتكوين ملف التعريف الخاص بك بنجاح، يجب أن تعرف، كحد أدنى، قيمك المكافئة للمعلومات التالية.

- اسم المضيف أو عنوان IP العام الخاص بمركز الشبكة الخاصة الظاهرية (10.48.66.109) (VPN)
- اسم المجموعة (RemoteClient)
- كلمة مرور المجموعة (Cisco)
- اسم المستخدم (joe)

قم بتحرير الملف باستخدام معلوماتك بحيث يكون مماثلا لما يلي.

```
[main]
Description=Connection to the corporate
Host=10.48.66.109
AuthType=1
GroupName=RemoteClient
GroupPwd=cisco
EnableISPConnect=0
ISPConnectType=0
=ISPConnect
=ISPCommand
Username=joe
SaveUserPassword=0
EnableBackup=0
=BackupServer
EnableNat=0
CertStore=0
=CertName
=CertPath
=CertSubjectName
```

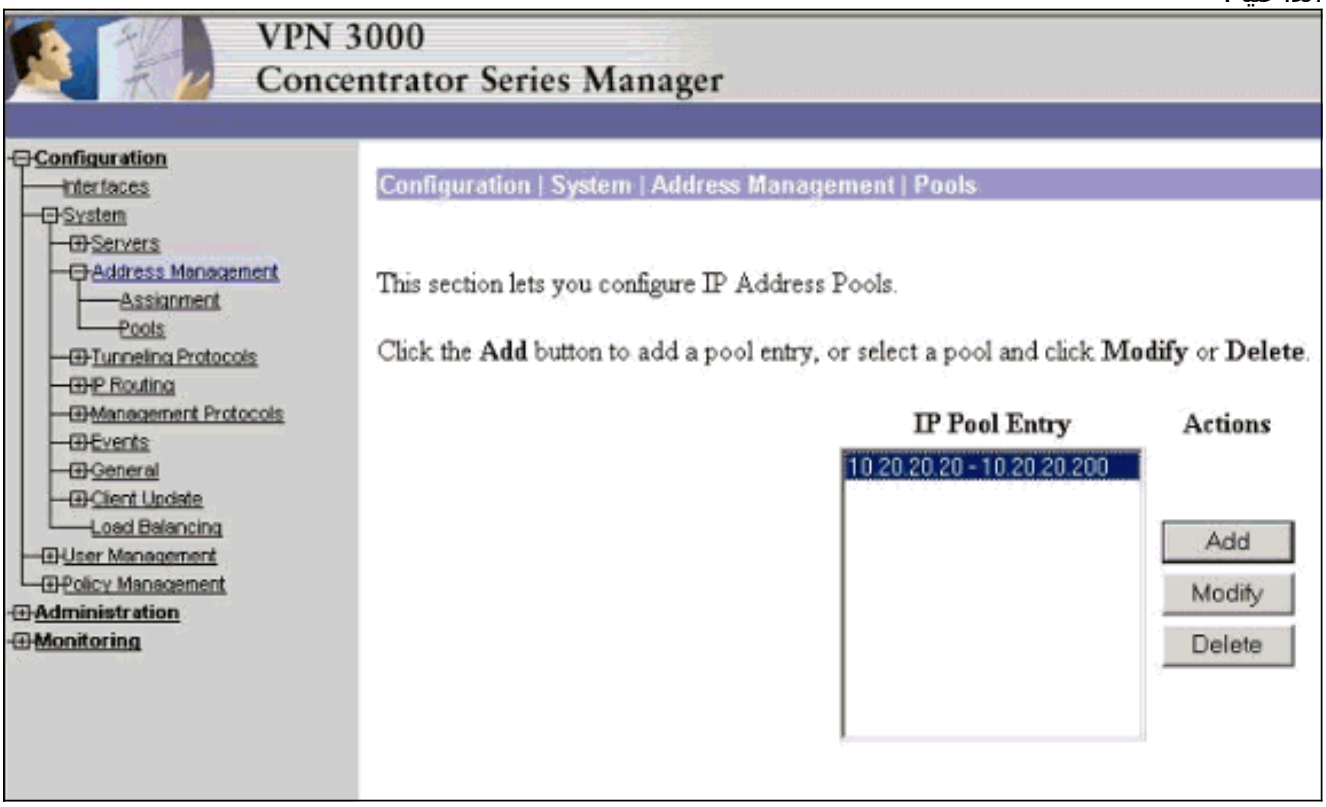
```
CertSerialHash=0000000000000000000000000000000000000000
DHGroup=2
ForceKeepAlives=0
```

تكوين مركز VPN

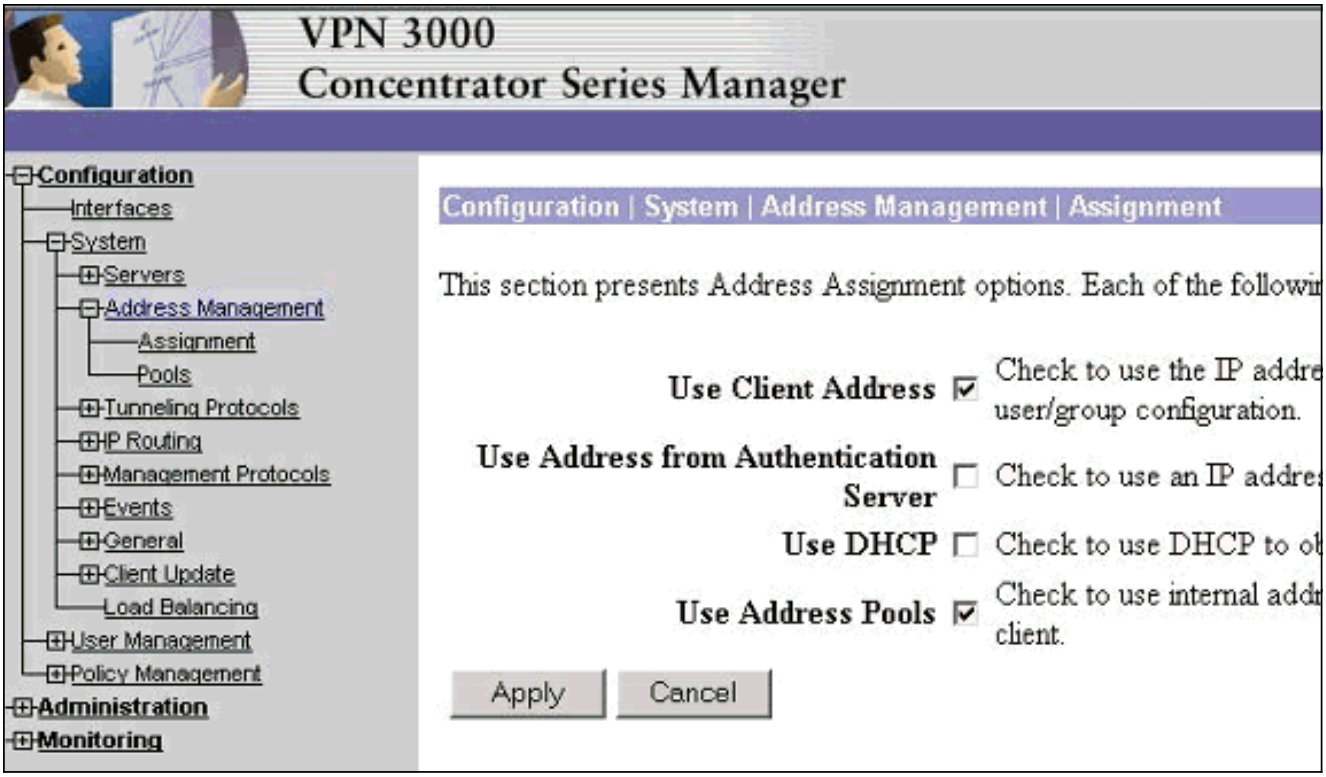
أستخدم الخطوات التالية لتكوين مركز VPN.

ملاحظة: نظرا لقيود المساحة، تظهر لقطات الشاشة المناطق الجزئية أو ذات الصلة فقط.

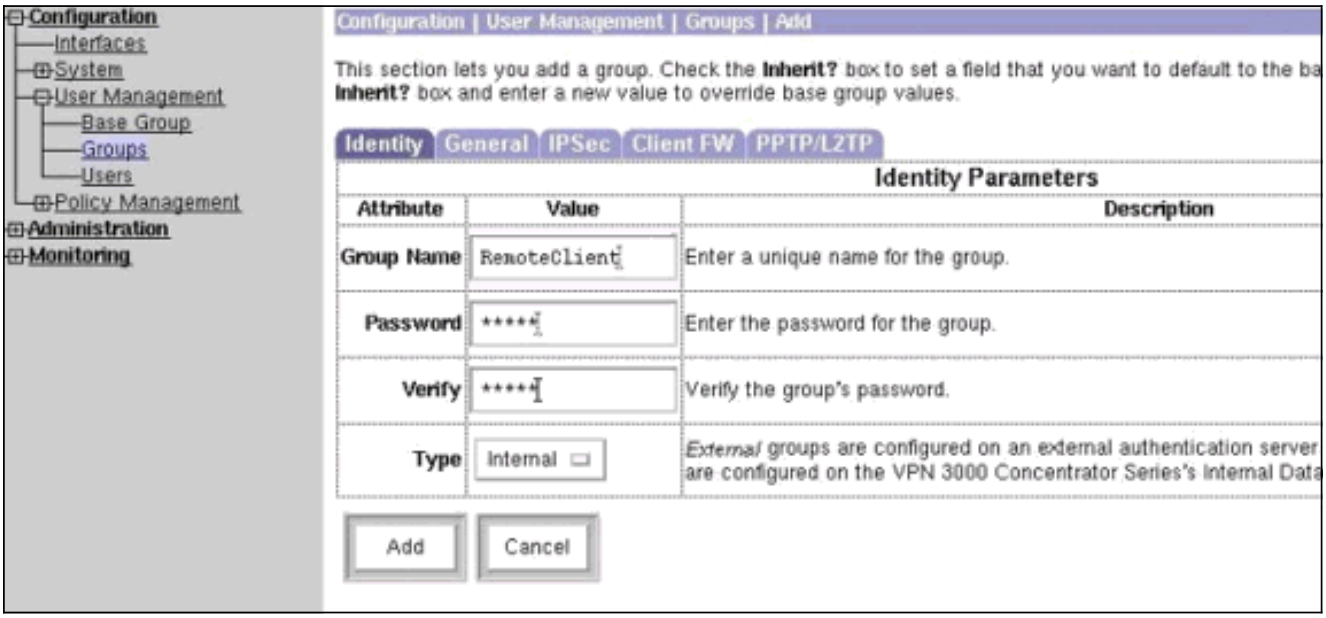
1. قم بتعيين مجموعة العناوين. لتخصيص نطاق متاح من عناوين IP، قم بتوجيه متصفح إلى الواجهة الداخلية لمركز تركيز الشبكة الخاصة الظاهرية (VPN) وحدد **تكوين > نظام > إدارة العناوين >تجمعات**. انقر فوق **إضافة (Add)**. حدد نطاق عناوين IP التي لا تتعارض مع أي أجهزة أخرى على الشبكة الداخلية.



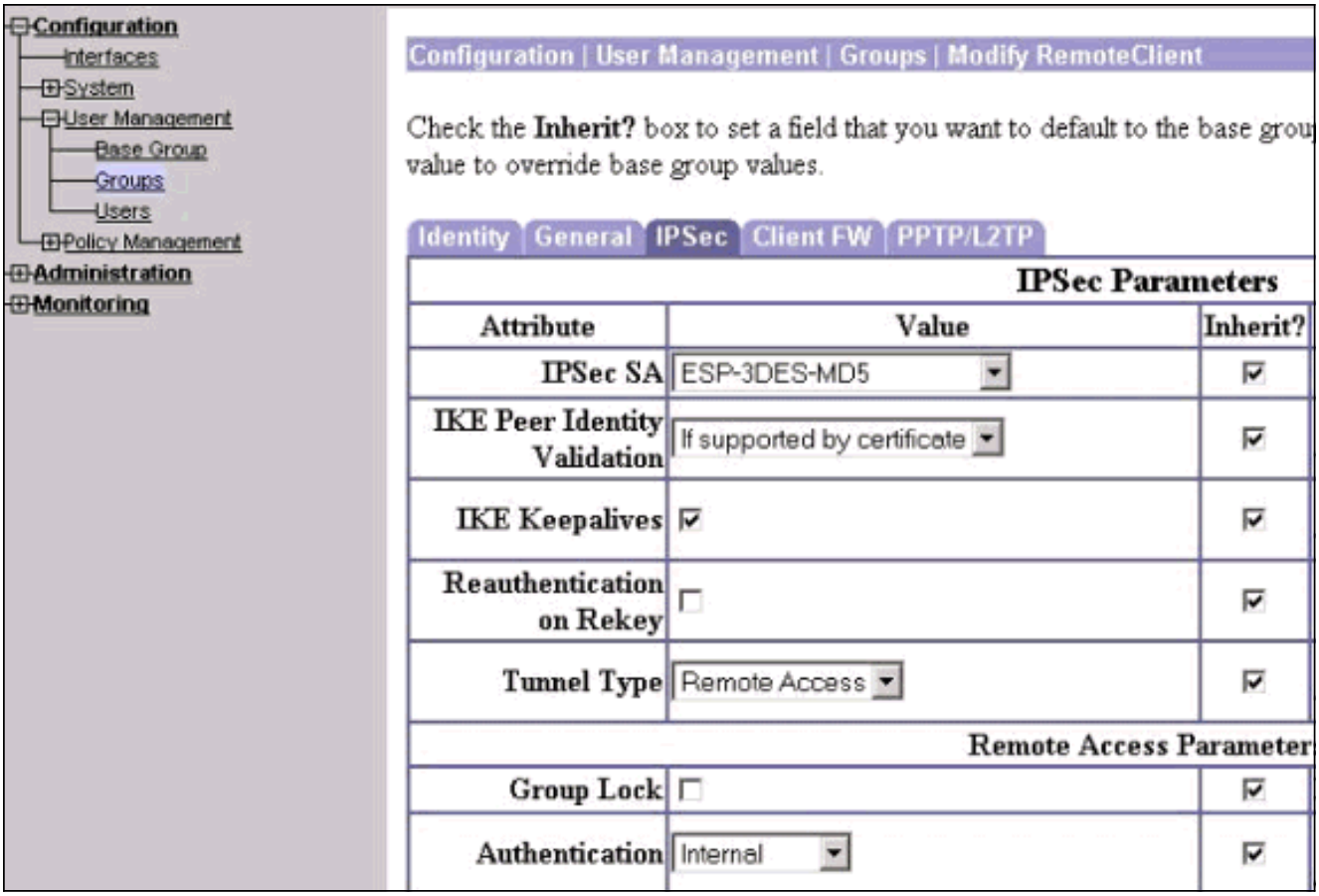
2. لإخبار مركز الشبكة الخاصة الظاهرية (VPN) باستخدام المجموعة، حدد **التكوين > النظام > إدارة العناوين > التعيين**، وحدد المربع **إستخدام تجمعات العناوين**، ثم انقر فوق **تطبيق**.



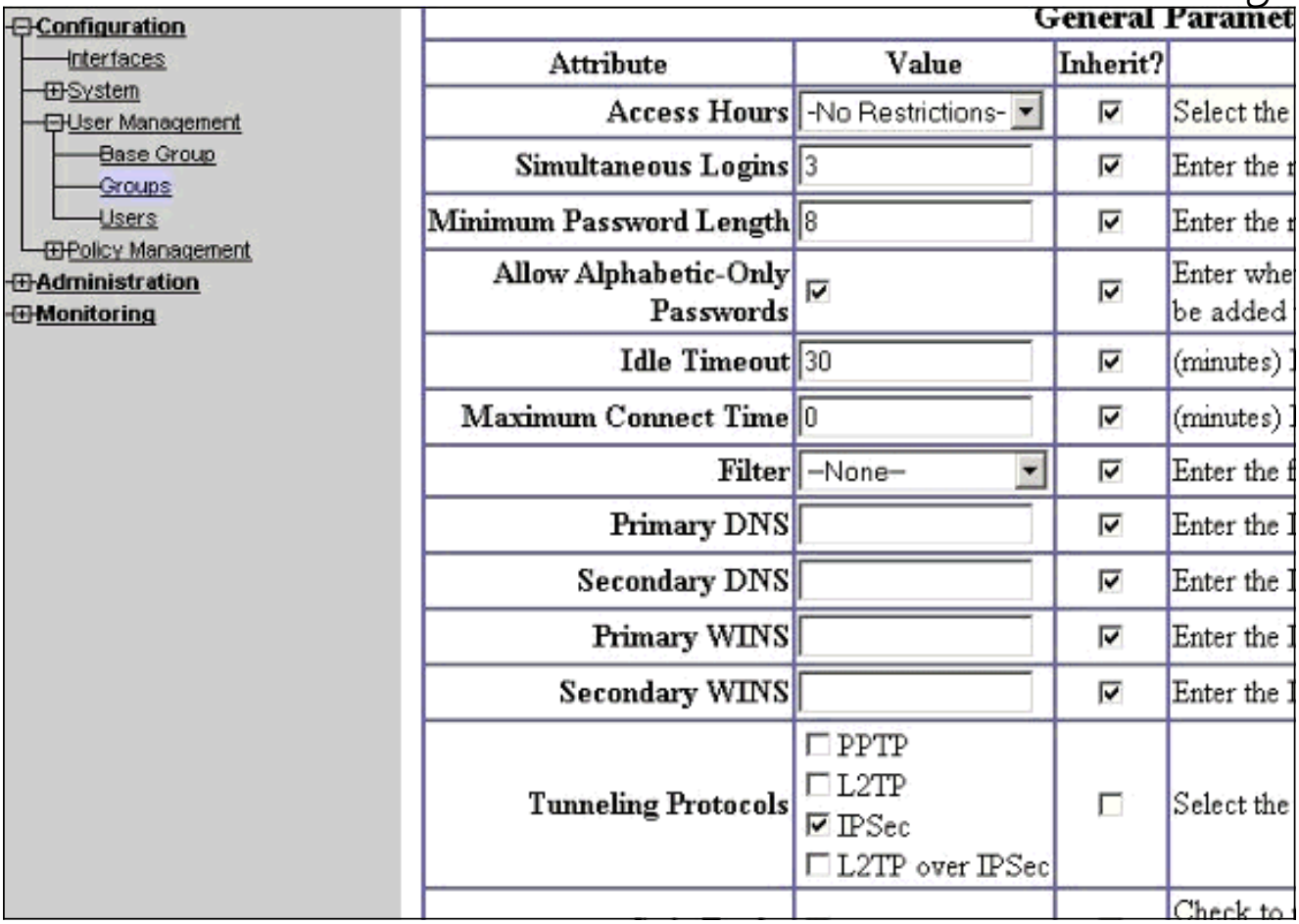
3. إضافة مجموعة وكلمة مرور. حدد **تكوين > إدارة المستخدم > مجموعات**، ثم انقر فوق **إضافة مجموعة**. أدخل المعلومات الصحيحة، ثم انقر فوق **إضافة** لإرسال المعلومات.يستخدم هذا المثال مجموعة تسمى "RemoteClient" بكلمة مرور من "cisco".



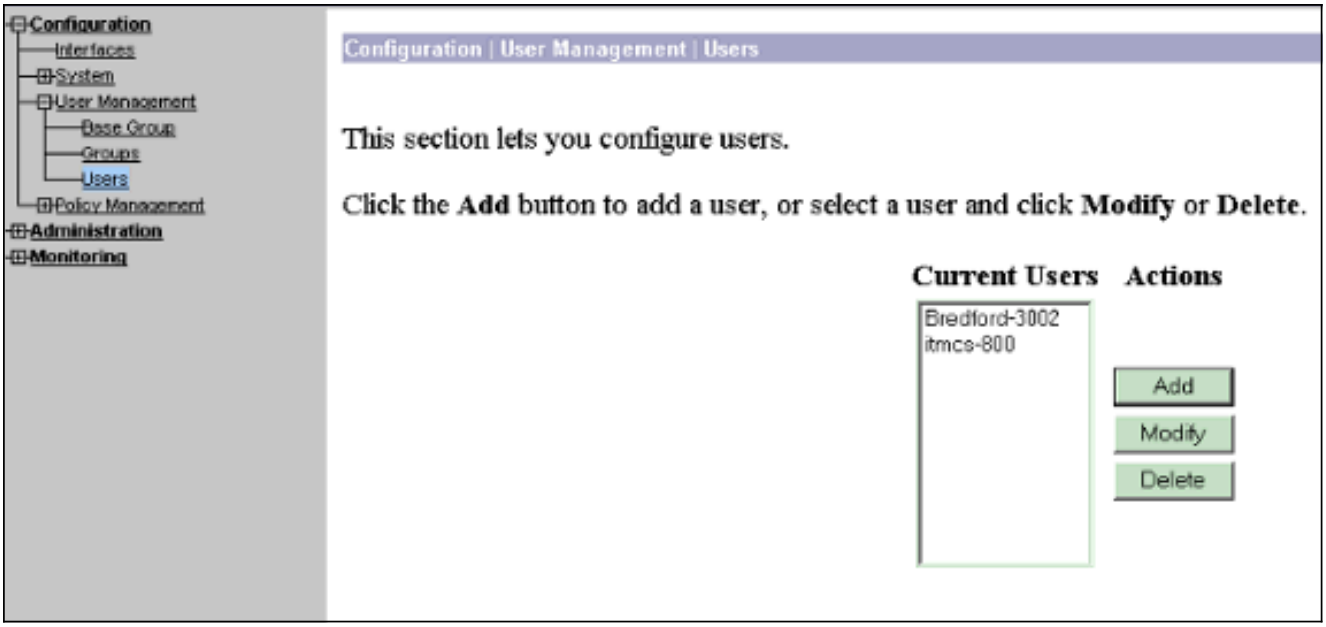
4. في علامة تبويب IPSec الخاصة بالمجموعة، تحقق من تعيين المصادقة على **داخلي**.



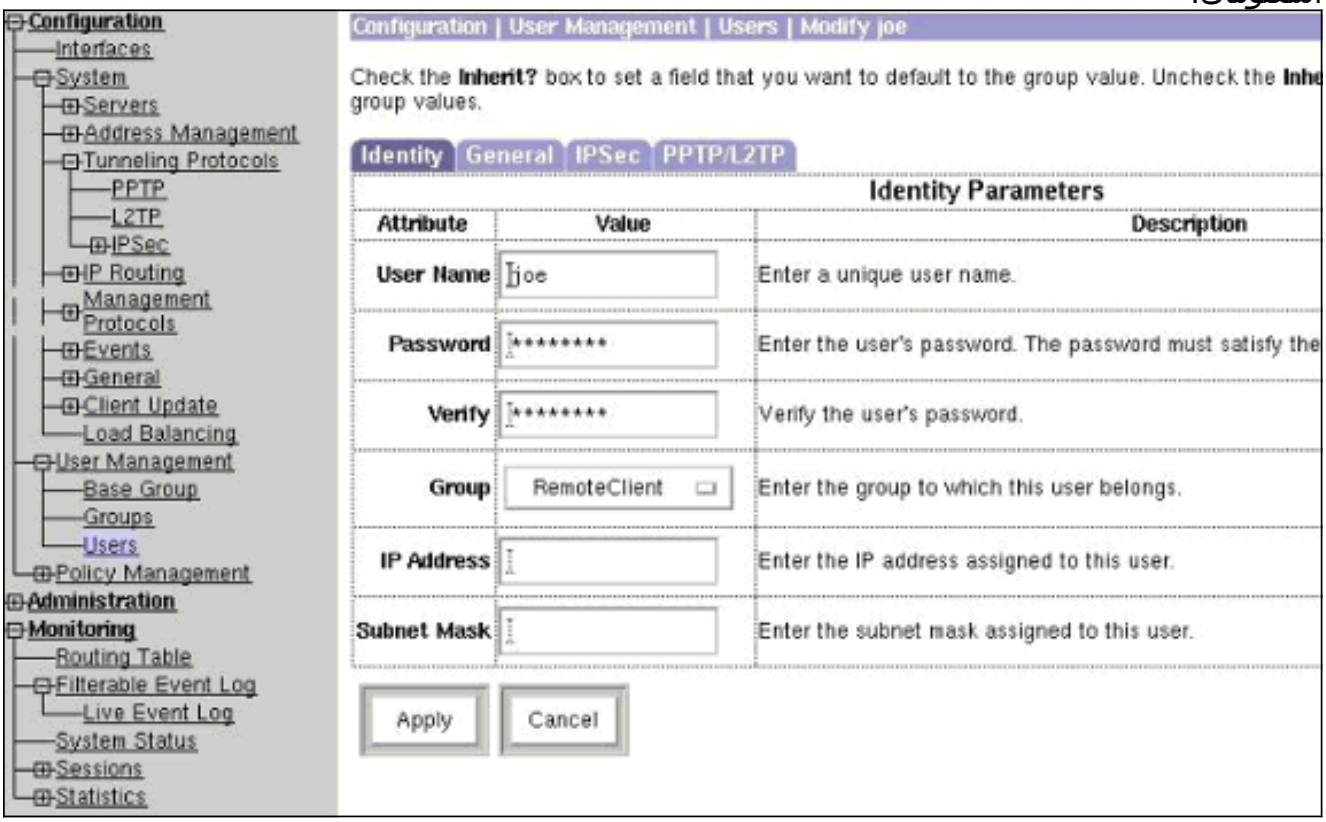
5. على علامة التبويب "عام" الخاصة بالمجموعة، تحقق من تحديد **IPSec** كبروتوكولات نفق.



6. لإضافة المستخدم إلى مركز الشبكة الخاصة الظاهرية (VPN)، حدد **تكوين > إدارة المستخدم > المستخدمين**، ثم انقر فوق **إضافة**.



7. أدخل المعلومات الصحيحة للمجموعة، ثم انقر فوق **تطبيق** لإرسال المعلومات.



التحقق من الصحة

إمكانية التوصيل بمركز الشبكة الخاصة الظاهرية (VPN)

الآن بعد تكوين عميل الشبكة الخاصة الظاهرية (VPN) ومكثف الشبكة الخاصة الظاهرية (VPN)، يجب أن يعمل التوصيف الجديد على الاتصال بمركز الشبكة الخاصة الظاهرية (VPN).

```
cholera]: /etc/CiscoSystemsVPNClient > vpnclient connect toCORPORATE] 91
                                    (Cisco Systems VPN Client Version 3.5 (Rel
.Copyright (C) 1998-2001 Cisco Systems, Inc. All Rights Reserved
                                    Client Type(s): Solaris
```

```
Running on: SunOS 5.6 Generic_105181-11 sun4u

                                    .Initializing the IPSec link
                  Contacting the security gateway at 10.48.66.109
                                            .Authenticating user
                         ...User Authentication for toCORPORATE

                                    .Enter Username and Password

                                                 :[Username [Joe
                                                    :[] Password
                  Contacting the security gateway at 10.48.66.109
                                            .Your link is secure
                                       .IPSec tunnel information
                                     Client address: 10.20.20.20
                                    Server address: 10.48.66.109
                                       Encryption: 168-bit 3-DES
                                        Authentication: HMAC-MD5
                                            IP Compression: None
                                    .NAT passthrough is inactive
                                    .Local LAN Access is disabled

                                                              Z^
                                                         Suspended

                                        cholera]: /etc/CiscoSystemsVPNClient > bg]
                                            & vpnclient connect toCORPORATE    [1]
                         (The process is made to run as background process)

                      cholera]: /etc/CiscoSystemsVPNClient > vpnclient disconnect]

                                    (Cisco Systems VPN Client Version 3.5 (Rel
                .Copyright (C) 1998-2001 Cisco Systems, Inc. All Rights Reserved
                                                 Client Type(s): Solaris
                                    Running on: SunOS 5.6 Generic_105181-11 sun4u

                                        .Your IPSec link has been disconnected
                                                .Disconnecting the IPSEC link
                                    < cholera]: /etc/CiscoSystemsVPNClient]
Exit -56                                vpnclient connect toCORPORATE    [1]

                                    < cholera]: /etc/CiscoSystemsVPNClient]
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

تصحيح الأخطاء

لتمكين تصحيح الأخطاء، أستخدم الأمر **ipseclog**. ويرد أدناه مثال على ذلك.

```
cholera]: /etc/CiscoSystemsVPNClient > ipseclog /tmp/clientlog]
```

تصحيح الأخطاء على العميل عند التوصيل بالمركز

```
cholera]: /etc/CiscoSystemsVPNClient > cat /tmp/clientlog]
```

```
  Sev=Info/4     CLI/0x43900002  01/25/2002  17:08:49.821      1
                                                  :Started vpnclient
                       (Cisco Systems VPN Client Version 3.5 (Rel
.Copyright (C) 1998-2001 Cisco Systems, Inc. All Rights Reserved
                                                  Client Type(s): Solaris
                     Running on: SunOS 5.6 Generic_105181-11 sun4u

Sev=Info/4     CVPND/0x4340000F  01/25/2002  17:08:49.855      2
                                                    :Started cvpnd
                       (Cisco Systems VPN Client Version 3.5 (Rel
.Copyright (C) 1998-2001 Cisco Systems, Inc. All Rights Reserved
                                                  Client Type(s): Solaris
                     Running on: SunOS 5.6 Generic_105181-11 sun4u

Sev=Info/4     IPSEC/0x43700013  01/25/2002  17:08:49.857      3
                            Delete internal key with SPI=0xb0f0d0c0

Sev=Info/4     IPSEC/0x4370000C  01/25/2002  17:08:49.857      4
                              Key deleted by SPI 0xb0f0d0c0

Sev=Info/4     IPSEC/0x43700013  01/25/2002  17:08:49.858      5
                            Delete internal key with SPI=0x637377d3

Sev=Info/4     IPSEC/0x4370000C  01/25/2002  17:08:49.858      6
                              Key deleted by SPI 0x637377d3

Sev=Info/4     IPSEC/0x43700013  01/25/2002  17:08:49.859      7
                            Delete internal key with SPI=0x9d4d2b9d

Sev=Info/4     IPSEC/0x4370000C  01/25/2002  17:08:49.859      8
                              Key deleted by SPI 0x9d4d2b9d

Sev=Info/4     IPSEC/0x43700013  01/25/2002  17:08:49.859      9
                            Delete internal key with SPI=0x5facd5bf

Sev=Info/4     IPSEC/0x4370000C  01/25/2002  17:08:49.860     10
                              Key deleted by SPI 0x5facd5bf

Sev=Info/4     IPSEC/0x43700009  01/25/2002  17:08:49.860     11
                                IPSec driver already started

Sev=Info/4     IPSEC/0x43700014  01/25/2002  17:08:49.861     12
                                                 Deleted all keys

Sev=Info/4     IPSEC/0x43700014  01/25/2002  17:08:49.861     13
                                                 Deleted all keys

Sev=Info/4     IPSEC/0x43700009  01/25/2002  17:08:49.862     14
                                IPSec driver already started

Sev=Info/4     IPSEC/0x43700009  01/25/2002  17:08:49.863     15
                                IPSec driver already started

Sev=Info/4     IPSEC/0x43700014  01/25/2002  17:08:49.863     16
                                                 Deleted all keys

   Sev=Info/4     CM/0x43100002  01/25/2002  17:08:50.873     17
                                       Begin connection process

   Sev=Info/4     CM/0x43100004  01/25/2002  17:08:50.883     18
                          Establish secure connection using Ethernet

   Sev=Info/4     CM/0x43100026  01/25/2002  17:08:50.883     19
                           "Attempt connection with server "10.48.66.109
```

```
Sev=Info/6     IKE/0x4300003B  01/25/2002  17:08:50.883     20
       .Attempting to establish a connection with 10.48.66.109

Sev=Info/4     IKE/0x43000013  01/25/2002  17:08:51.099     21
 SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID) to
                                                  10.48.66.109

Sev=Info/4     IPSEC/0x43700009  01/25/2002  17:08:51.099     22
                                      IPSec driver already started

Sev=Info/4     IPSEC/0x43700014  01/25/2002  17:08:51.100     23
                                                 Deleted all keys

Sev=Info/5     IKE/0x4300002F  01/25/2002  17:08:51.400     24
                     Received ISAKMP packet: peer = 10.48.66.109

Sev=Info/4     IKE/0x43000014  01/25/2002  17:08:51.400     25
,RECEIVING <<< ISAKMP OAK AG (SA, KE, NON, ID, HASH, VID, VID, VID
                                          VID) from 10.48.66.109

Sev=Info/5     IKE/0x43000059  01/25/2002  17:08:51.400     26
          Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100

Sev=Info/5     IKE/0x43000001  01/25/2002  17:08:51.400     27
                             Peer is a Cisco-Unity compliant peer

Sev=Info/5     IKE/0x43000059  01/25/2002  17:08:51.400     28
                             Vendor ID payload = 09002689DFD6B712

Sev=Info/5     IKE/0x43000059  01/25/2002  17:08:51.400     29
          Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100

Sev=Info/5     IKE/0x43000001  01/25/2002  17:08:51.400     30
                                           Peer supports DPD

Sev=Info/5     IKE/0x43000059  01/25/2002  17:08:51.400     31
          Vendor ID payload = 1F07F70EAA6514D3B0FA96542A500301

Sev=Info/4     IKE/0x43000013  01/25/2002  17:08:51.505     32
(SENDING >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT
                                             to 10.48.66.109

Sev=Info/5     IKE/0x4300002F  01/25/2002  17:08:51.510     33
                     Received ISAKMP packet: peer = 10.48.66.109

Sev=Info/4     IKE/0x43000014  01/25/2002  17:08:51.511     34
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 10.48.66.109

 Sev=Info/4     CM/0x43100015  01/25/2002  17:08:51.511     35
                                       Launch xAuth application

 Sev=Info/4     CM/0x43100017  01/25/2002  17:08:56.333     36
                                     xAuth application returned

Sev=Info/4     IKE/0x43000013  01/25/2002  17:08:56.334     37
    SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 10.48.66.109

Sev=Info/5     IKE/0x4300002F  01/25/2002  17:08:56.636     38
                     Received ISAKMP packet: peer = 10.48.66.109

Sev=Info/4     IKE/0x43000014  01/25/2002  17:08:56.637     39
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 10.48.66.109
```

```
 Sev=Info/4     CM/0x4310000E  01/25/2002  17:08:56.637     40
           Established Phase 1 SA.  1 Phase 1 SA in the system

Sev=Info/4     IKE/0x43000013  01/25/2002  17:08:56.639     41
    SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 10.48.66.109

Sev=Info/4     IKE/0x43000013  01/25/2002  17:08:56.639     42
    SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 10.48.66.109

Sev=Info/5     IKE/0x4300002F  01/25/2002  17:08:56.645     43
                    Received ISAKMP packet: peer = 10.48.66.109

Sev=Info/4     IKE/0x43000014  01/25/2002  17:08:56.646     44
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 10.48.66.109

Sev=Info/5     IKE/0x43000010  01/25/2002  17:08:56.646     45
          , :MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS
                                          value = 10.20.20.20

Sev=Info/5     IKE/0x4300000D  01/25/2002  17:08:56.646     46
          , :MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD
                                          value = 0x00000000

Sev=Info/5     IKE/0x4300000D  01/25/2002  17:08:56.646     47
              , :MODE_CFG_REPLY: Attribute = MODECFG_UNITY_PFS
                                          value = 0x00000000

Sev=Info/5     IKE/0x4300000E  01/25/2002  17:08:56.646     48
              ,MODE_CFG_REPLY: Attribute = APPLICATION_VERSION
      value = Cisco Systems, Inc./VPN 3000 Concentrator Series
      Version 3.1.Rel built by vmurphy on Aug 06 2001 13:47:37

 Sev=Info/4     CM/0x43100019  01/25/2002  17:08:56.648     49
                                    Mode Config data received

Sev=Info/5     IKE/0x43000055  01/25/2002  17:08:56.651     50
,Received a key request from Driver for IP address 10.48.66.109
                                          GW IP = 10.48.66.109

Sev=Info/4     IKE/0x43000013  01/25/2002  17:08:56.652     51
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 10.48.66.109

Sev=Info/5     IKE/0x43000055  01/25/2002  17:08:56.653     52
,Received a key request from Driver for IP address 10.10.10.255
                                          GW IP = 10.48.66.109

Sev=Info/4     IKE/0x43000013  01/25/2002  17:08:56.653     53
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 10.48.66.109

Sev=Info/5     IKE/0x4300002F  01/25/2002  17:08:56.663     54
                    Received ISAKMP packet: peer = 10.48.66.109

Sev=Info/4     IKE/0x43000014  01/25/2002  17:08:56.663     55
(RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:STATUS_RESP_LIFETIME
                                          from 10.48.66.109

Sev=Info/5     IKE/0x43000044  01/25/2002  17:08:56.663     56
          RESPONDER-LIFETIME notify has value of 86400 seconds

Sev=Info/5     IKE/0x43000046  01/25/2002  17:08:56.663     57
  This SA has already been alive for 6 seconds, setting expiry
                                    to 86394 seconds from now

Sev=Info/5     IKE/0x4300002F  01/25/2002  17:08:56.666     58
```

```
                    Received ISAKMP packet: peer = 10.48.66.109

  Sev=Info/4     IKE/0x43000014  01/25/2002  17:08:56.666     59
           ,RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID
                 NOTIFY:STATUS_RESP_LIFETIME) from 10.48.66.109

  Sev=Info/5     IKE/0x43000044  01/25/2002  17:08:56.667     60
           RESPONDER-LIFETIME notify has value of 28800 seconds

  Sev=Info/4     IKE/0x43000013  01/25/2002  17:08:56.667     61
              SENDING >>> ISAKMP OAK QM *(HASH) to 10.48.66.109

  Sev=Info/5     IKE/0x43000058  01/25/2002  17:08:56.667     62
       = Loading IPsec SA (Message ID = 0x4CEF4B32 OUTBOUND SPI
                          (0x5EAD41F5 INBOUND SPI = 0xE66C759A

  Sev=Info/5     IKE/0x43000025  01/25/2002  17:08:56.668     63
                          Loaded OUTBOUND ESP SPI: 0x5EAD41F5

  Sev=Info/5     IKE/0x43000026  01/25/2002  17:08:56.669     64
                          Loaded INBOUND ESP SPI: 0xE66C759A

   Sev=Info/4     CM/0x4310001A  01/25/2002  17:08:56.669     65
                          One secure connection established

  Sev=Info/5     IKE/0x4300002F  01/25/2002  17:08:56.674     66
                    Received ISAKMP packet: peer = 10.48.66.109

  Sev=Info/4     IKE/0x43000014  01/25/2002  17:08:56.675     67
           ,RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID
                 NOTIFY:STATUS_RESP_LIFETIME) from 10.48.66.109

  Sev=Info/5     IKE/0x43000044  01/25/2002  17:08:56.675     68
           RESPONDER-LIFETIME notify has value of 28800 seconds

  Sev=Info/4     IKE/0x43000013  01/25/2002  17:08:56.675     69
              SENDING >>> ISAKMP OAK QM *(HASH) to 10.48.66.109

  Sev=Info/5     IKE/0x43000058  01/25/2002  17:08:56.675     70
       = Loading IPsec SA (Message ID = 0x88E9321A OUTBOUND SPI
                          (0x333B4239 INBOUND SPI = 0x6B040746

  Sev=Info/5     IKE/0x43000025  01/25/2002  17:08:56.677     71
                          Loaded OUTBOUND ESP SPI: 0x333B4239

  Sev=Info/5     IKE/0x43000026  01/25/2002  17:08:56.677     72
                          Loaded INBOUND ESP SPI: 0x6B040746

   Sev=Info/4     CM/0x43100022  01/25/2002  17:08:56.678     73
                          .Additional Phase 2 SA established

Sev=Info/4     IPSEC/0x43700014  01/25/2002  17:08:57.752     74
                                             Deleted all keys

Sev=Info/4     IPSEC/0x43700010  01/25/2002  17:08:57.752     75
                                  Created a new key structure

Sev=Info/4     IPSEC/0x4370000F  01/25/2002  17:08:57.752     76
                    Added key with SPI=0x5ead41f5 into key list

Sev=Info/4     IPSEC/0x43700010  01/25/2002  17:08:57.753     77
                                  Created a new key structure

Sev=Info/4     IPSEC/0x4370000F  01/25/2002  17:08:57.753     78
```

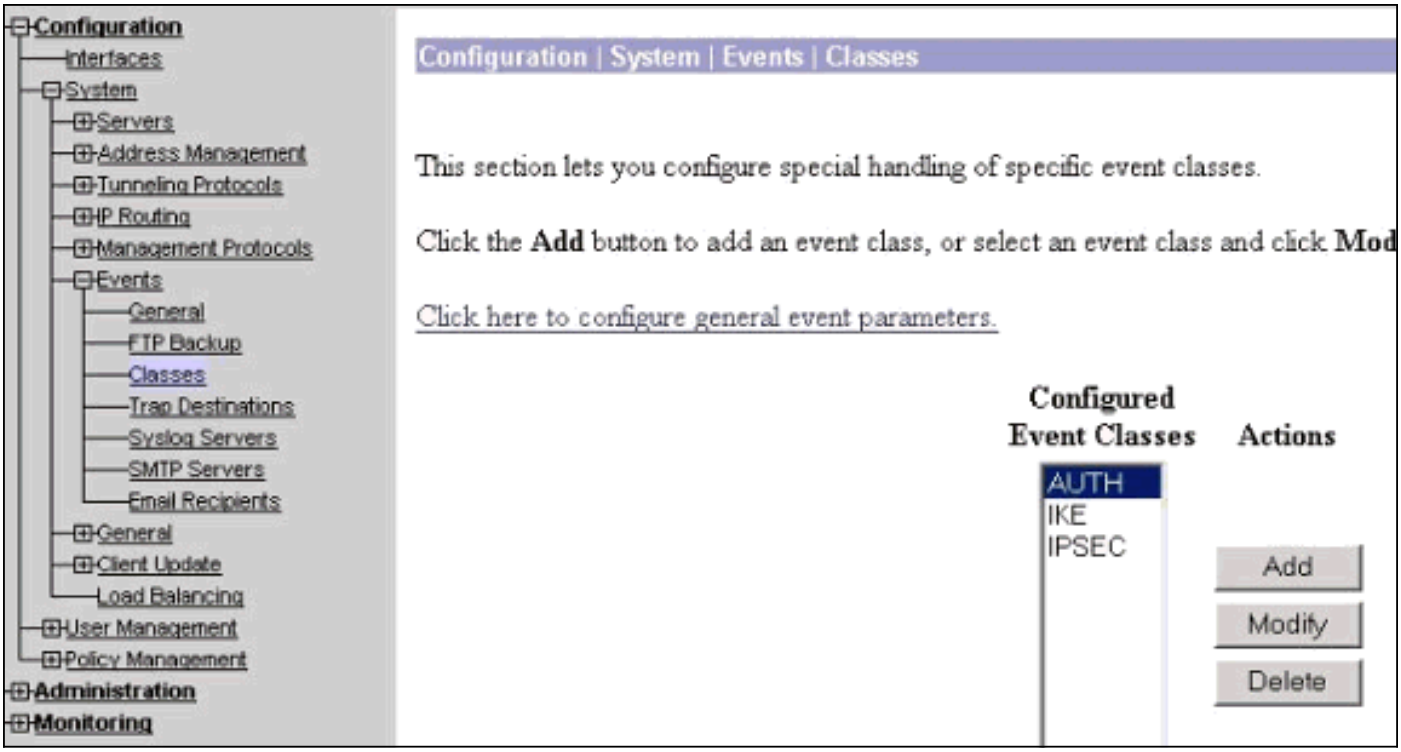
```
                        Added key with SPI=0xe66c759a into key list

   Sev=Info/4     IPSEC/0x43700010  01/25/2002  17:08:57.754     79
                                     Created a new key structure

   Sev=Info/4     IPSEC/0x4370000F  01/25/2002  17:08:57.754     80
                        Added key with SPI=0x333b4239 into key list

   Sev=Info/4     IPSEC/0x43700010  01/25/2002  17:08:57.754     81
                                     Created a new key structure

   Sev=Info/4     IPSEC/0x4370000F  01/25/2002  17:08:57.755     82
                        Added key with SPI=0x6b040746 into key list

     Sev=Info/6     IKE/0x4300003D  01/25/2002  17:09:13.752     83
             Sending DPD request to 10.48.66.109, seq# = 2948297981

     Sev=Info/4     IKE/0x43000013  01/25/2002  17:09:13.752     84
            (SENDING >>> ISAKMP OAK INFO *(HASH, NOTIFY:DPD_REQUEST
                                                 to 10.48.66.109

     Sev=Info/5     IKE/0x4300002F  01/25/2002  17:09:13.758     85
                        Received ISAKMP packet: peer = 10.48.66.109

     Sev=Info/4     IKE/0x43000014  01/25/2002  17:09:13.758     86
              (RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:DPD_ACK
                                               from 10.48.66.109

     Sev=Info/5     IKE/0x4300003F  01/25/2002  17:09:13.759     87
    ,Received DPD ACK from 10.48.66.109, seq# received = 2948297981
                                     seq# expected = 2948297981



                              debug on the client when disconnecting
     Sev=Info/4     CLI/0x43900002  01/25/2002  17:09:16.366     88
                                              :Started vpnclient
                          (Cisco Systems VPN Client Version 3.5 (Rel
   .Copyright (C) 1998-2001 Cisco Systems, Inc. All Rights Reserved
                                     Client Type(s): Solaris
                       Running on: SunOS 5.6 Generic_105181-11 sun4u

      Sev=Info/4     CM/0x4310000A  01/25/2002  17:09:16.367     89
                                   Secure connections terminated

     Sev=Info/5     IKE/0x43000018  01/25/2002  17:09:16.367     90
(Deleting IPsec SA: (OUTBOUND SPI = 333B4239 INBOUND SPI = 6B040746

     Sev=Info/4     IKE/0x43000013  01/25/2002  17:09:16.368     91
           SENDING >>> ISAKMP OAK INFO *(HASH, DEL) to 10.48.66.109

     Sev=Info/5     IKE/0x43000018  01/25/2002  17:09:16.369     92
(Deleting IPsec SA: (OUTBOUND SPI = 5EAD41F5 INBOUND SPI = E66C759A

     Sev=Info/4     IKE/0x43000013  01/25/2002  17:09:16.369     93
           SENDING >>> ISAKMP OAK INFO *(HASH, DEL) to 10.48.66.109

     Sev=Info/4     IKE/0x43000013  01/25/2002  17:09:16.370     94
           SENDING >>> ISAKMP OAK INFO *(HASH, DEL) to 10.48.66.109

      Sev=Info/4     CM/0x43100013  01/25/2002  17:09:16.371     95
                  .Phase 1 SA deleted cause by DEL_REASON_RESET_SADB
                                   Phase 1 SA currently in the system 0
```

```
Sev=Info/5     CM/0x43100029  01/25/2002  17:09:16.371     96
                                          Initializing CVPNDrv

Sev=Info/6     CM/0x43100035  01/25/2002  17:09:16.371     97
          :Tunnel to headend device 10.48.66.109 disconnected
                                      duration: 0 days 0:0:20

Sev=Info/5     CM/0x43100029  01/25/2002  17:09:16.375     98
                                          Initializing CVPNDrv

Sev=Info/5     IKE/0x4300002F  01/25/2002  17:09:16.377     99
                   Received ISAKMP packet: peer = 10.48.66.109

Sev=Warning/2  IKE/0x83000061  01/25/2002  17:09:16.377    100
      Attempted incoming connection from 10.48.66.109. Inbound
                                    .connections are not allowed

Sev=Info/4     IPSEC/0x43700013  01/25/2002  17:09:17.372    101
                             Delete internal key with SPI=0x6b040746

Sev=Info/4     IPSEC/0x43700013  01/25/2002  17:09:17.372    102
                             Delete internal key with SPI=0x333b4239

Sev=Info/4     IPSEC/0x43700013  01/25/2002  17:09:17.373    103
                             Delete internal key with SPI=0xe66c759a

Sev=Info/4     IPSEC/0x43700013  01/25/2002  17:09:17.373    104
                             Delete internal key with SPI=0x5ead41f5

Sev=Info/4     IPSEC/0x43700014  01/25/2002  17:09:17.373    105
                                             Deleted all keys

Sev=Info/4     IPSEC/0x43700009  01/25/2002  17:09:17.374    106
                                IPSec driver already started

Sev=Info/4     IPSEC/0x43700014  01/25/2002  17:09:17.374    107
                                             Deleted all keys

Sev=Info/4     IPSEC/0x43700009  01/25/2002  17:09:17.375    108
                                IPSec driver already started

Sev=Info/4     IPSEC/0x43700014  01/25/2002  17:09:17.375    109
                                             Deleted all keys

Sev=Info/4     IPSEC/0x43700009  01/25/2002  17:09:17.375    110
                                IPSec driver already started

Sev=Info/4     IPSEC/0x43700014  01/25/2002  17:09:17.376    111
                                             Deleted all keys
```

تصحيح الأخطاء على مركز VPN

حدد **تشكيل > نظام > أحداث > فئات** لتشغيل تصحيح الأخطاء التالي إذا كان هناك فشل في اتصال الحدث.

- **المصادقة** - الخطورة للتسجيل من 1 إلى 13
- **IKE** - مستوى الخطورة للتسجيل من 1 إلى 6
- **IPSec** - مستوى الخطورة المطلوب تسجيلها من 1 إلى 6



يمكنك عرض السجل بتحديد **مراقبة > سجل الأحداث**.

معلومات ذات صلة

- صفحة دعم مركز Cisco VPN 3000 Series
- صفحة دعم عميل Cisco VPN 3000 Series
- صفحة دعم IPSec
- الدعم الفني - 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).