عميل Cisco VPN إلى مركز VPN 3000 مع مصادقة IPSec SDI (الخادم إصدار 3.3)

المحتويات

المقدمة

يمكن تكوين مركز Cisco VPN 3000 لمصادقة عملاء Cisco VPN من خلال خادم Security Dynamics International (SDI). يعمل مركز VPN 3000 كعميل SDI، حيث يتصل بخادم SDI على منفذ بروتوكول مخطط بيانات المستخدم (UDP) 5500. يوضح المستند التالي كيفية التأكد من أن خادم SDI ومجمع VPN 3000 وعميل Cisco VPN يعملون بشكل صحيح، ومن ثم كيفية تجميع المكونات. إذا لم يتم تكوين مركز VPN 3000 لديك بعد، فاستخدم الخطوات من تثبيت مركز VPN 3000 وتكوينه بدون SDI باستخدام واجهة سطر الأوامر (CLI) للتثبيت والتكوين الأساسيين. إذا كان قد تم تكوين مركز VPN 3000 مسبقا، فاتبع الخطوات لتعديل التكوين الموجود (بدون SDI).

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات أساسية خاصة لهذا المستند.

المكونات المستخدمة

تم تطوير هذه التهيئة واختبارها باستخدام إصدارات البرامج والمكونات المادية الواردة أدناه.

- خادم UNIX) SDI 3.3 و NT)
- مركز VPN 3000) 2.5.2)
- عميل شبكة VPN 2.5.2.a

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

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

معلومات أساسية

ينطبق هذا المستند على كل من عميل Cisco VPN 3000 (2.5.x) أو عميل Cisco VPN (3.x). مع الإصدار 3.0 والإصدارات الأحدث، يمكنك الآن تكوين خوادم SDI الفردية للمجموعات الفردية مقارنة بخادم SDI واحد المعرف بشكل عام والمستخدم بواسطة جميع المجموعات. ستستخدم تلك المجموعات التي ليس لديها خوادم SDI فردية تم تكوينها خادم SDI المحدد بشكل عام.

هناك ثلاثة أنواع من أوضاع رقم التعريف الشخصي (PIN) الجديدة في SDI. يدعم مركز VPN 3000 أول خيارين كما هو موضح أدناه.

- يختار المستخدم رقم تعريف شخصي جديد.
- يختار الخادم رقم تعريف شخصي (PIN) جديدا ويقوم بإعلام المستخدمين.
- يختار الخادم رقم تعريف شخصي (PIN) جديد ويقوم بإعلام المستخدمين، ويمكن للمستخدمين تغيير رقم التعريف الشخصي (PIN).

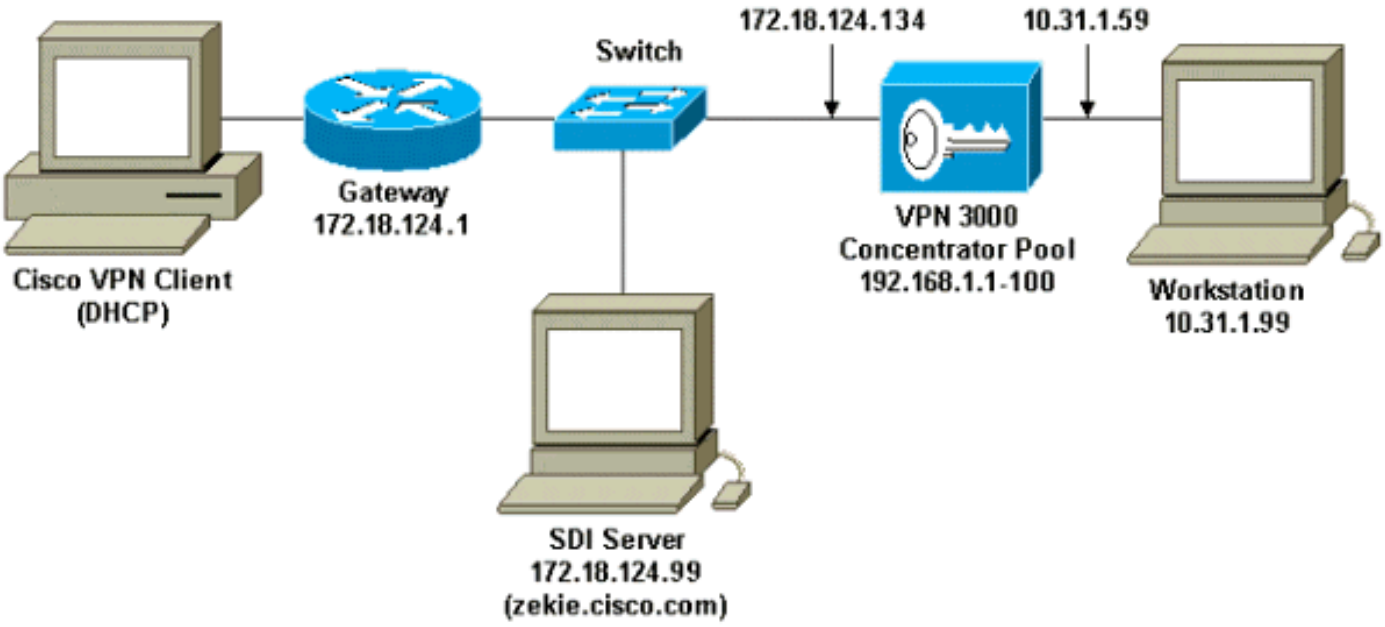
التكوين

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.



التكوينات

قم بتثبيت وتكوين مركز VPN 3000 بدون SDI

لقد قمنا بتكوين مركز VPN 3000 للمصادقة المحلية لمستخدم في مجموعة ما، ومن خلال القيام بذلك قبل إضافة SDI، يمكننا تحديد عمل IPSec بين عميل Cisco VPN ومجمع VPN 3000. لقد قمنا بمسح تكوين مركز VPN 3000 على منفذ وحدة التحكم من خلال الانتقال إلى **الإدارة > إعادة تمهيد النظام > إعادة تمهيد الجدول > إعادة التمهيد باستخدام تكوين المصنع/التكوين الافتراضي**.

بعد إعادة التشغيل، تم إجراء التكوين الأولي التالي:

تهيئة مركز VPN 3000 Concentrator

```
                                                Login: admin
                                                   :Password

                                    Welcome to
                                Cisco Systems
                            VPN 3000 Concentrator Series
                               Command Line Interface
                    .Copyright (C) 1998-2000 Cisco Systems, Inc

  Set the time on your device. The correct time is : --
                                                ,very important
                        so that logging and accounting entries are : --
                                                        .accurate

    :Enter the system time in the following format : --
   HH:MM:SS.  Example  21:30:00  for 9:30 PM       : --

                                                      Time <

                                                [ Quick -> [ 13:02:39

                                .Enter the date in the following format : --
                      MM/DD/YYYY  Example 06/12/1999  for June 12th : --
                                                            .1999

                                                      Date <
```

```
                                    [ Quick -> [ 10/09/2000

Set the time zone on your device. The correct time : --
                                                 zone is very
  important so that logging and accounting entries : --
                                                .are accurate

    Enter the time zone using the hour offset from : --
                                                       :GMT
      Kwajalein  -11 : Samoa    -10 : Hawaii : -12 : --
                                                  -9 : Alaska
         PST         -7 : MST       -6 : CST : -8  : --
                                                    -5 : EST
Atlantic    -3 : Brasilia  -2 : Mid-Atlantic : -4  : --
                                                  -1 : Azores
       GMT         +1 : Paris     +2 : Cairo : 0   : --
                                                  +3 : Kuwait
      Abu Dhabi   +5 : Karachi   +6 : Almaty : +4  : --
                                                +7 : Bangkok
      Singapore   +9 : Tokyo    +10 : Sydney : +8  : --
                                         .+11 : Solomon Is
                                    .Marshall Is : +12 : --

                                                 Time Zone <

                                         Quick -> [ -5 ] -5

                                      Enable DST Support (1
                                     Disable DST Support (2

                                              [ Quick -> [ 1

                    .This table shows current IP addresses

   Interface                    IP Address/Subnet Mask
                                                 MAC Address
-----------------------------------------------------------
                                    ----------------------
       Ethernet 1 - Private  |         0.0.0.0/0.0.0.0 |
                                                         |
       Ethernet 2 - Public   |         0.0.0.0/0.0.0.0 |
                                                         |

       Ethernet 3 - External |         0.0.0.0/0.0.0.0 |
                                                         |
-----------------------------------------------------------
                                    ----------------------

 ** .An address is required for the private interface **

                                         Enter IP Address <

               Quick Ethernet 1 -> [ 0.0.0.0 ] 10.31.1.59

                    ...Waiting for Network Initialization

                                        Enter Subnet Mask <

         Quick Ethernet 1 -> [ 255.0.0.0 ] 255.255.255.0

                                   Ethernet Speed 10 Mbps (1
                                  Ethernet Speed 100 Mbps (2
                 Ethernet Speed 10/100 Mbps Auto Detect (3
```

```
                                [ Quick Ethernet 1 -> [ 3

                           Enter Duplex - Half/Full/Auto (1
                              Enter Duplex - Full Duplex (2
                              Enter Duplex - Half Duplex (3

                                [ Quick Ethernet 1 -> [ 1

                    (Modify Ethernet 1 IP Address (Private (1
                     (Modify Ethernet 2 IP Address (Public (2
                   (Modify Ethernet 3 IP Address (External (3
                                Configure Expansion Cards (4
                             Save changes to Config file (5
                                                  Continue (6
                                                      Exit (7

                                                   Quick -> 2

                        .This table shows current IP addresses

   Interface                    IP Address/Subnet Mask
                                                  MAC Address
-----------------------------------------------------------
                                    ----------------------
 Ethernet 1 - Private  |      10.31.1.59/255.255.255.0 |
                                          |  00.90.A4.00.1C.B4
       Ethernet 2 - Public   |         0.0.0.0/0.0.0.0 |
                                                        |
       Ethernet 3 - External |         0.0.0.0/0.0.0.0 |
                                                        |
-----------------------------------------------------------
                                    ----------------------

                                         Enter IP Address <

          Quick Ethernet 2 -> [ 0.0.0.0 ] 172.18.124.134

                                        Enter Subnet Mask <

       Quick Ethernet 2 -> [ 255.255.0.0 ] 255.255.255.0

                                     Ethernet Speed 10 Mbps (1
                                    Ethernet Speed 100 Mbps (2
                 Ethernet Speed 10/100 Mbps Auto Detect (3

                                [ Quick Ethernet 2 -> [ 3

                           Enter Duplex - Half/Full/Auto (1
                              Enter Duplex - Full Duplex (2
                              Enter Duplex - Half Duplex (3

                                [ Quick Ethernet 2 -> [ 1

                    (Modify Ethernet 1 IP Address (Private (1
                     (Modify Ethernet 2 IP Address (Public (2
                   (Modify Ethernet 3 IP Address (External (3
                                Configure Expansion Cards (4
                             Save changes to Config file (5
                                                  Continue (6
                                                      Exit (7

                                                   Quick -> 6
```

```
                .Assign a system name to this device : --

                                                System Name <

                                              Quick -> vpn3000

  Specify a local DNS server, which lets you enter : --
                                                        hostnames
       .rather than IP addresses while configuring : --

                                                DNS Server <

                                          [ Quick -> [ 0.0.0.0

           Enter your Internet domain name; e.g., : --
                                              yourcompany.com

                                                       Domain <

                                                       <- Quick

                                           Default Gateway <

                                        Quick -> 172.18.124.1

        .Configure protocols and encryption options : --
         This table shows current protocol settings : --

          |         PPTP         |        L2TP
          ----------------------------------------------
          |       Enabled        |       Enabled       |
          |  No Encryption Req   |  No Encryption Req  |
          ----------------------------------------------

                                          Enable  PPTP (1
                                          Disable PPTP (2

                                           [ Quick -> [ 1

                                PPTP Encryption Required (1
                                  No Encryption Required (2

                                                [ Quick -> [ 2

                                          Enable  L2TP (1
                                          Disable L2TP (2

                                           [ Quick -> [ 1
                                L2TP Encryption Required (1
                                  No Encryption Required (2

                                                [ Quick -> [ 2

                                         Enable  IPSec (1
                                         Disable IPSec (2

                                           [ Quick -> [ 1

    Configure address assignment for PPTP, L2TP and : --
                                                        .IPSec

           Enable Client Specified Address Assignment (1
         Disable Client Specified Address Assignment (2
```

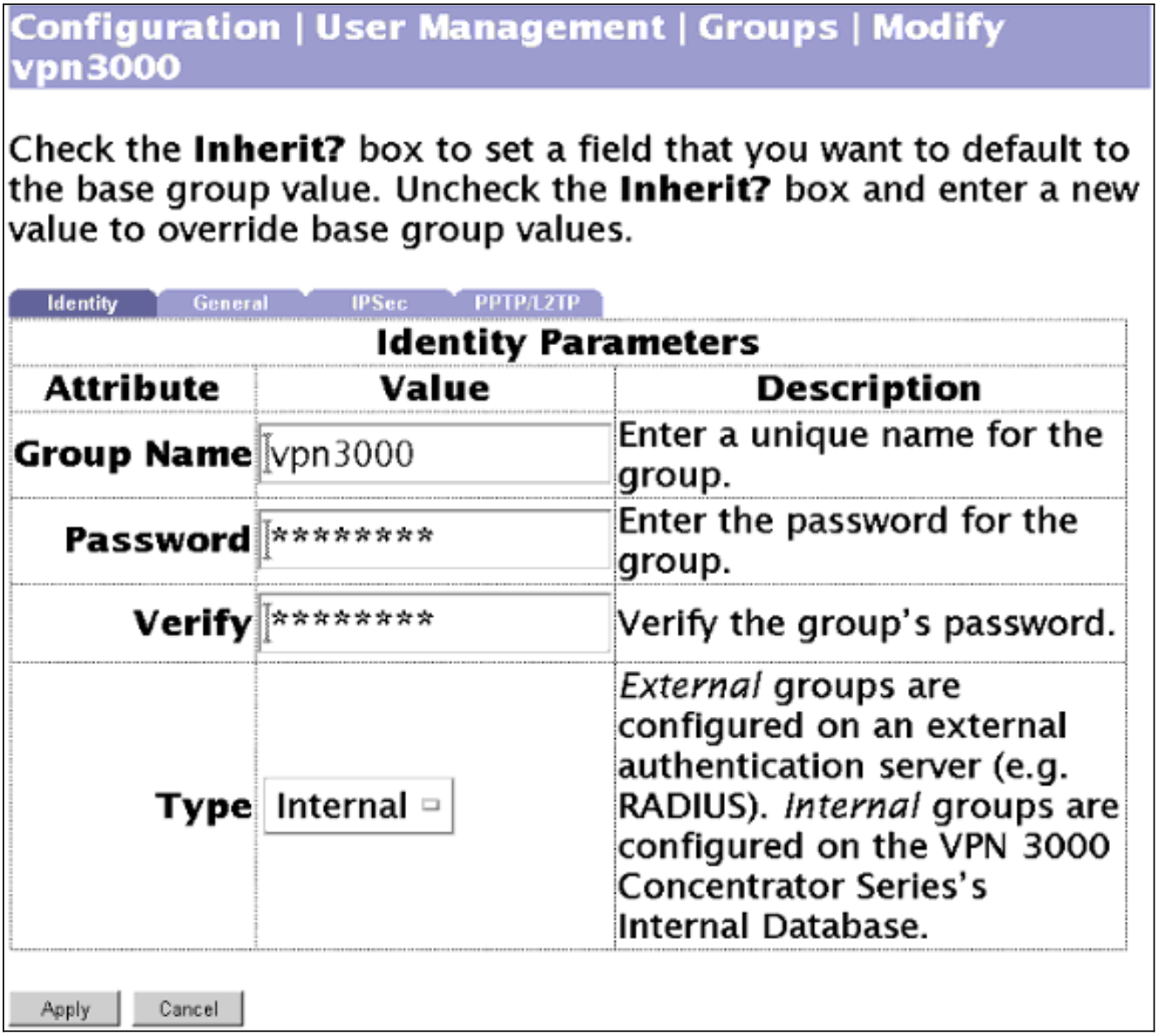
```
                                          [ Quick -> [ 2

                  Enable Per User Address Assignment (1
                 Disable Per User Address Assignment (2

                                          [ Quick -> [ 2

                      Enable DHCP Address Assignment (1
                     Disable DHCP Address Assignment (2

                                          [ Quick -> [ 2

            Enable Configured Pool Address Assignment (1
           Disable Configured Pool Address Assignment (2

                                       Quick -> [ 2 ] 1

                   Configured Pool Range Start Address <

                                     Quick -> 192.168.1.1

                     Configured Pool Range End Address <

                     Quick -> [ 0.0.0.0 ] 192.168.1.100

                  Specify how to authenticate users : --

                       Internal Authentication Server (1
                         RADIUS Authentication Server (2
                      NT Domain Authentication Server (3
                            SDI Authentication Server (4
                                             Continue (5

                                       Quick -> [ 1 ] 1

        Current Users
-----------------------------------------------------
                                    ----------------------
           No Users
-----------------------------------------------------
                                    ----------------------

                                          Add a User (1
                                       Delete a User (2
                                            Continue (3

                                           Quick -> 1

                                          User Name <

                                     Quick -> 37297304

                                          Password <

                                    ********* <- Quick
                                   ********* <- Verify

        Current Users
-----------------------------------------------------
                                    ----------------------
              |                           37297304 .1 |
                                                      |
-----------------------------------------------------
                                    ----------------------
```

```
                                                  Add a User (1
                                               Delete a User (2
                                                    Continue (3

                                                  Quick -> 3

                                              IPSec Group Name <

                                                Quick -> vpn3000

                                             IPSec Group Password <

                                                 ******** <- Quick
                                               ******** <- Verify

We strongly recommend that you change the password : --
                                                  .for user admin

                                             Reset Admin Password <

                                                 [ ***** ] <- Quick
                                                          <- Verify

                                          Goto Main Configuration Menu (1
                                           Save changes to Config file (2
                                                               Exit (3

                                                  Quick -> 2

                                          Goto Main Configuration Menu (1
                                           Save changes to Config file (2
                                                               Exit (3

                                                  Quick -> 3

                                                               Done
```

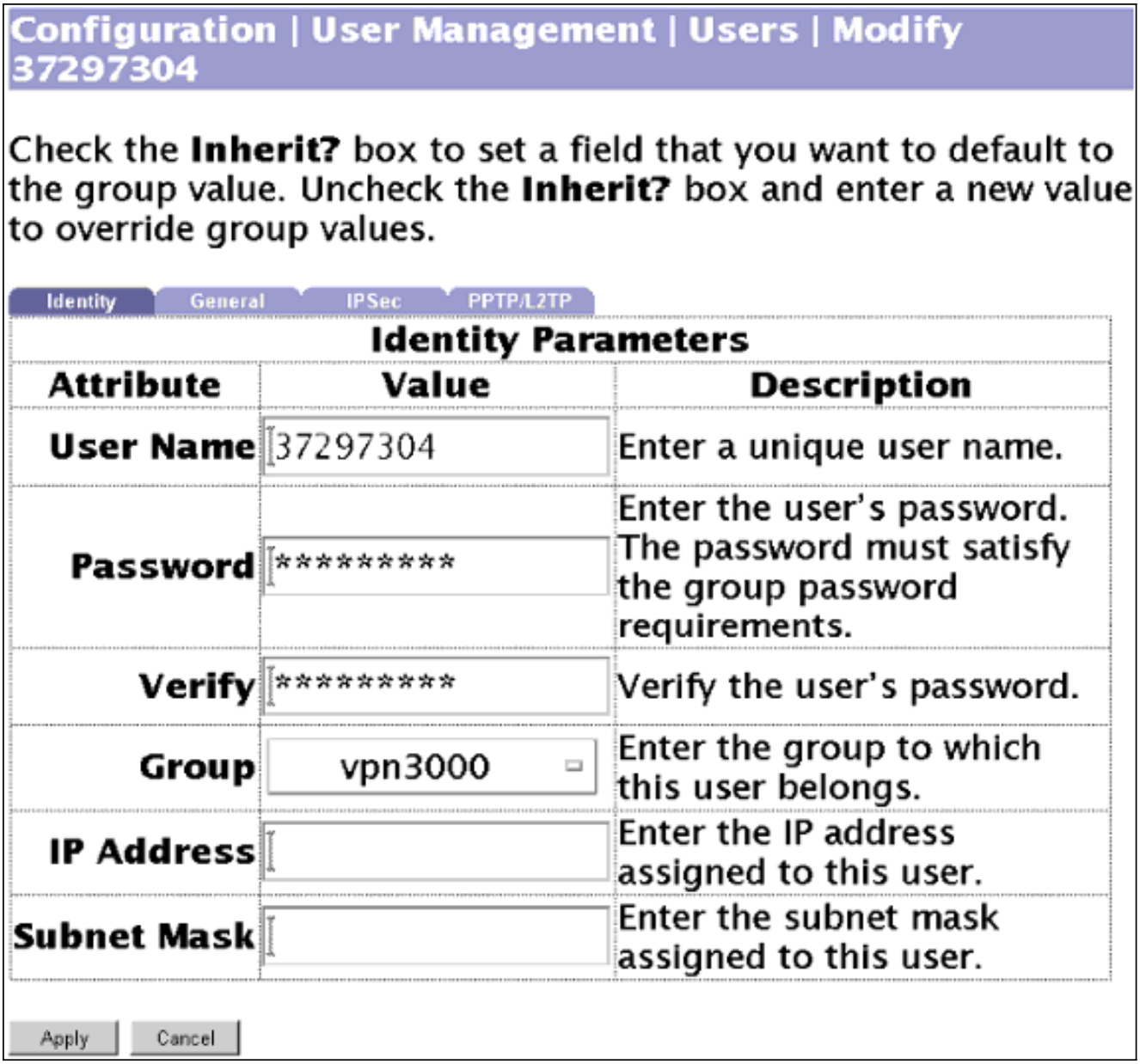
تعديل التكوين الموجود (بدون SDI)

إذا كان قد تم تكوين مركز VPN 3000 من قبل، فسيتم إستخدام الشاشات التالية للتحقق من إعدادات المجموعة والمستخدم و IPSec/IKE:

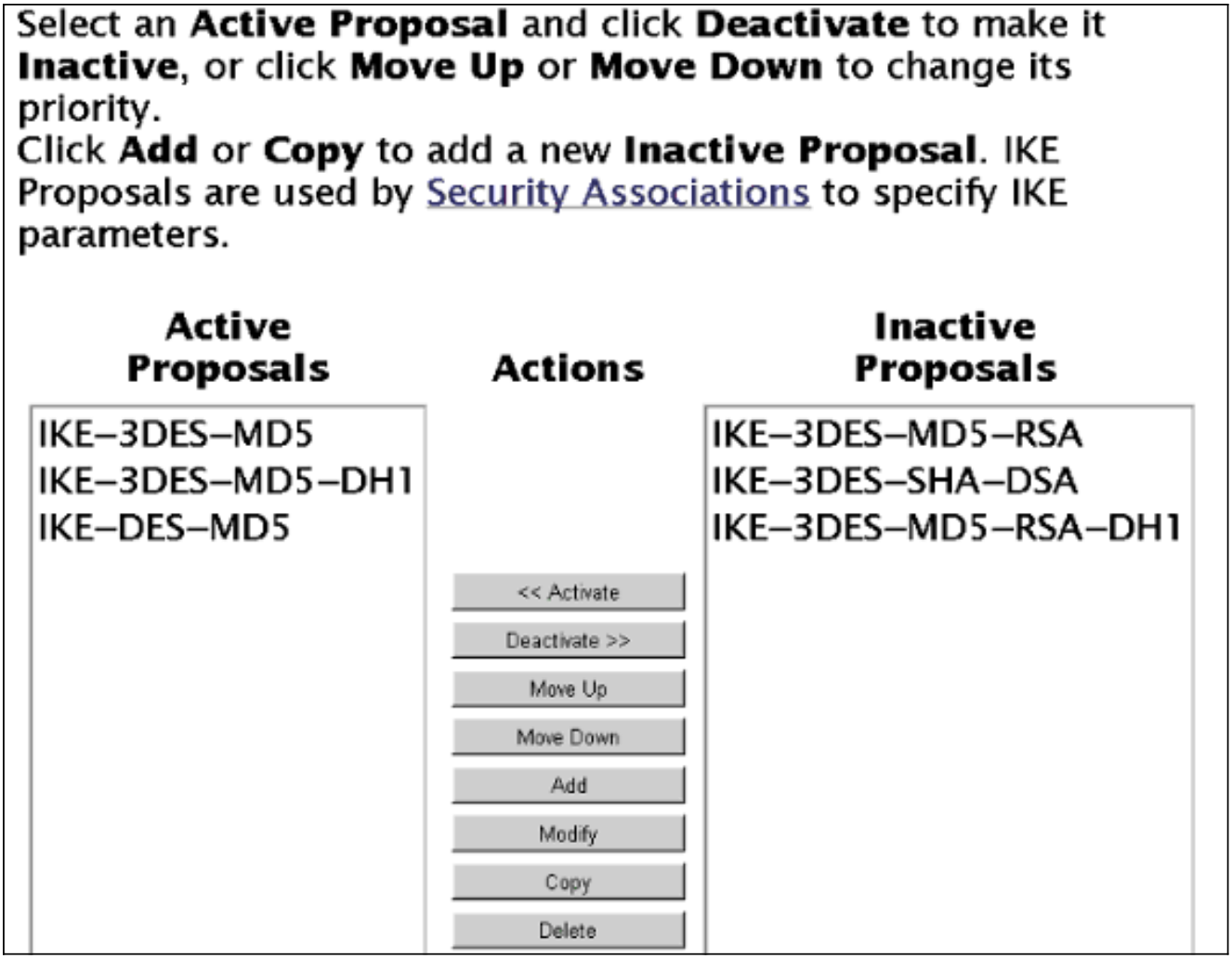
1. أستخدم هذه الشاشة لإضافة مجموعة بمصادقة محلية:



2. أستخدم هذه الشاشة لإضافة مستخدم إلى المجموعة بمصادقة محلية:



3. أستخدم شاشة عرض IPSec > عرض IKE لإضافة إعدادات IKE (الإعدادات الموضحة هي إعدادات النظام الافتراضية):



إختبار عميل Cisco VPN ومجمع VPN 3000 بدون SDI

بعد تعديل التكوين الموجود على مركز VPN 3000، قمنا بتثبيت عميل Cisco VPN وتكوينه اتصال جديد للإنهاء في 172.18.124.134 (الواجهة العامة للمتمركز). كانت معلومات وصول مجموعتنا "vpn3000" (اسم المجموعة) وكلمة مرور المجموعة هي كلمة المرور للمجموعة. عندما ننقر على **Connect**، كان اسم المستخدم هو "37297304" (اسم المستخدم) وكلمة مرور المستخدم هي كلمة مرور المستخدم (المخزنة محليا على مركز VPN 3000؛ لا يتضمن SDI بعد). راجع تصحيح أخطاء IPSec الجيد مع المصادقة المحلية لتصحيح IKE و iKEDBG و iKeddecode و IPSec و IPSECDBG و IPSECDECODE.

تشغيل خادم SDI للاختبار دون مركز VPN 3000

(UNIX (Solaris

1. على خادم SDI، قم بإنشاء حساب أكثر تكلفة باستخدام أداة Solaris Admintool.يجب أن يبدو إدخال etc/passwd/ كما يلي:
```
sditest:x:76:10::/local/0/sditest:/local/0/opt/ace/prog/sdshell
```
ملاحظة: تعتمد القيم والمسارات إلى الدليل الرئيسي للمستخدم و "sdshell" على النظام.
2. قم بتعيين رمز مميز للتعريف.
3. جرب إنشاء شبكة عن بعد داخل مضيف UNIX كحل. يطلب منك المضيف كلمة مرور UNIX ورمز المرور. وبعد المصادقة، يمكنك هذا المحول من الدخول إلى الجهاز المضيف.

مايكروسوفت ويندوز إن تي

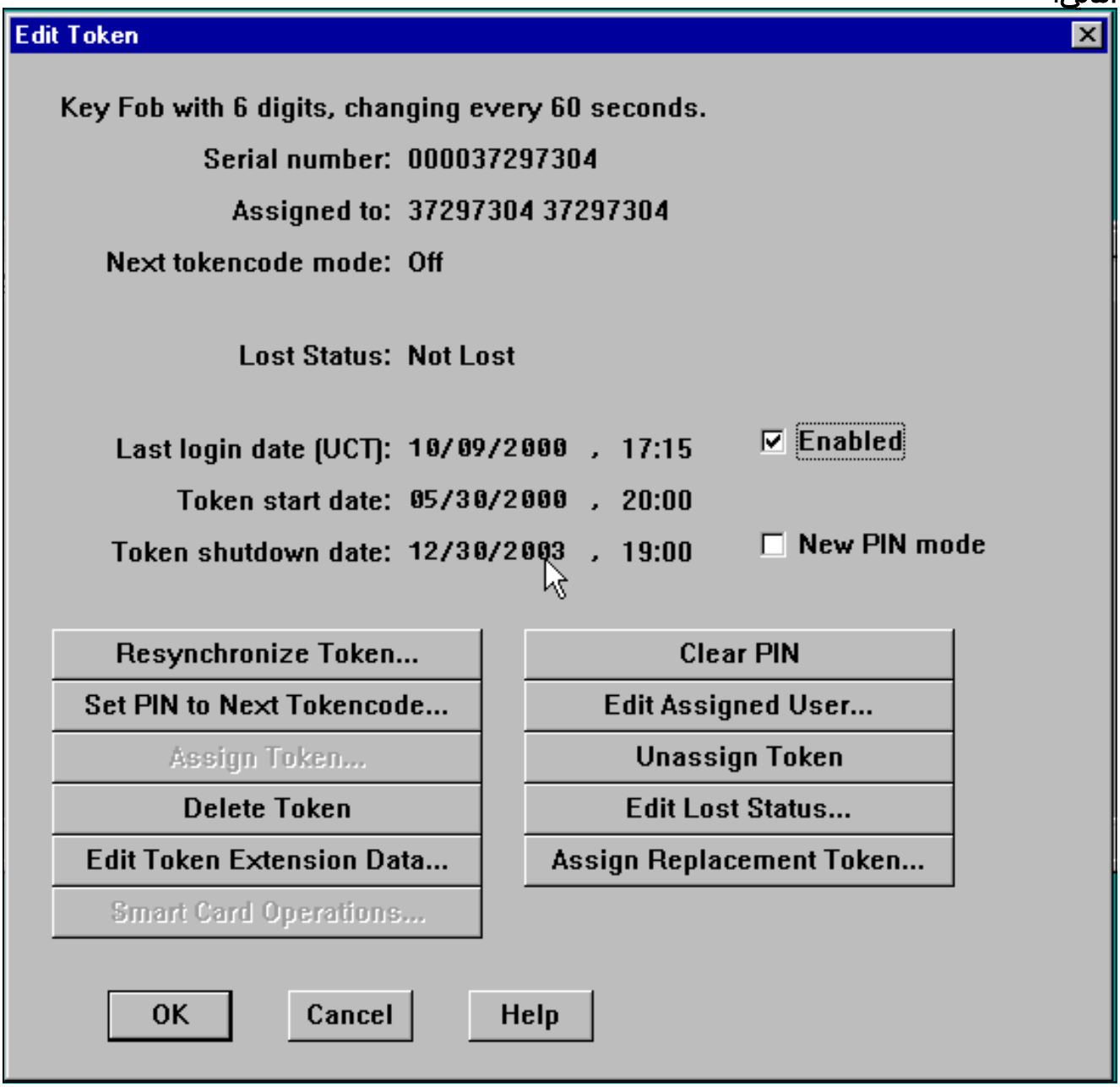
1. قم بتثبيت عامل SecureSight.

2. حدد **برامج > SecureSight > إختبار المصادقة**.

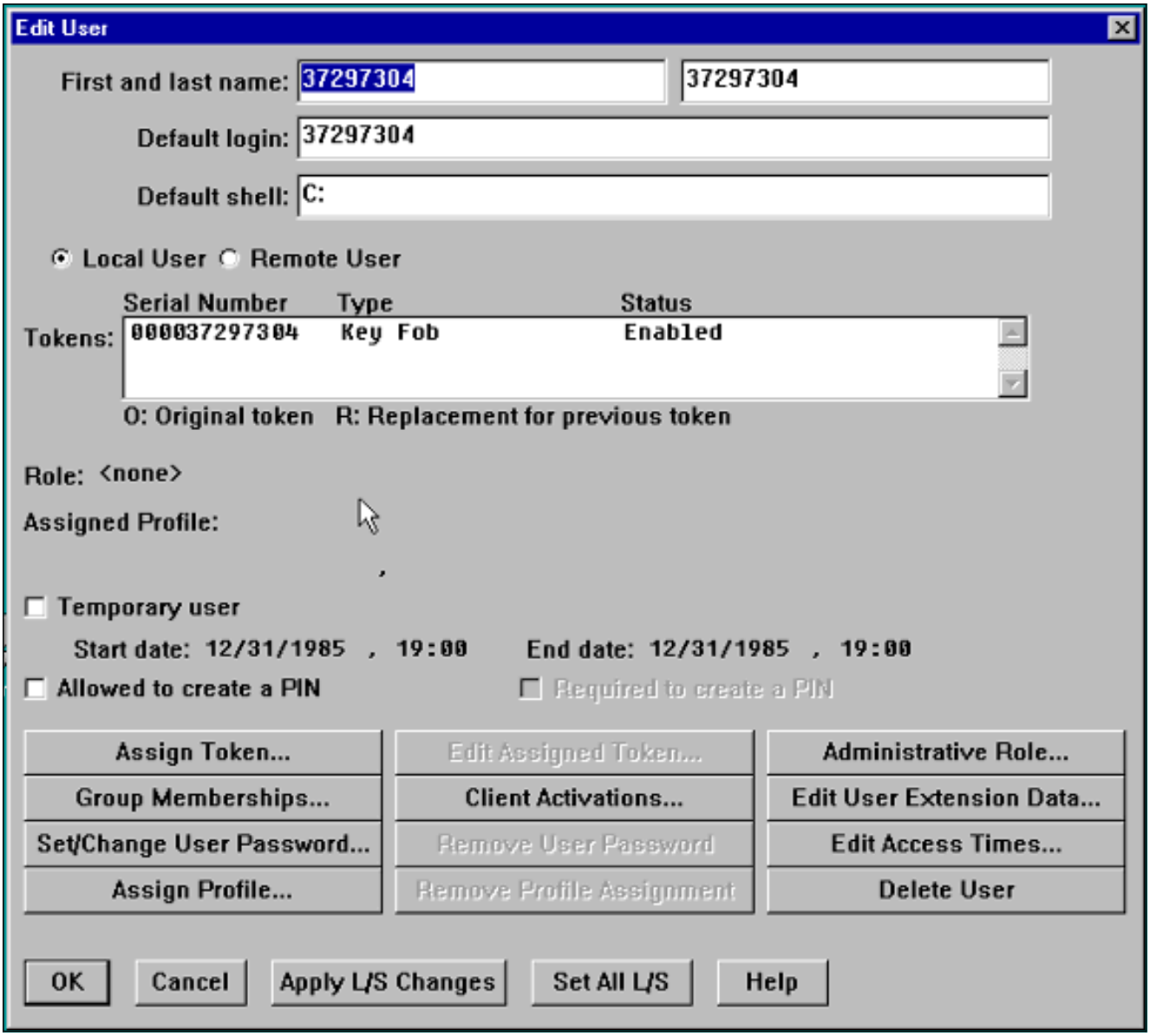
تكوين SDI/User للتحدث إلى مركز VPN 3000

أستخدم الخطوات التالية لتكوين SDI/User للحديث مع مركز VPN 3000:

1. على شاشة رمز تحرير خادم SDI المميز، تحقق من أن الرمز المميز "ممكن" وليس في وضع PIN الجديد.
2. انقر فوق **إعادة مزامنة الرمز المميز وتعيين PIN على الرمز المميز التالي**.



3. في شاشة تحرير المستخدم، قم بتعيين رمز مميز للمستخدم، وتحقق من عدم تحديد "السماح بإنشاء رقم تعريف شخصي (PIN)".
4. انقر فوق عمليات تنشيط العميل وتحقق من تضمين مركز VPN 3000.



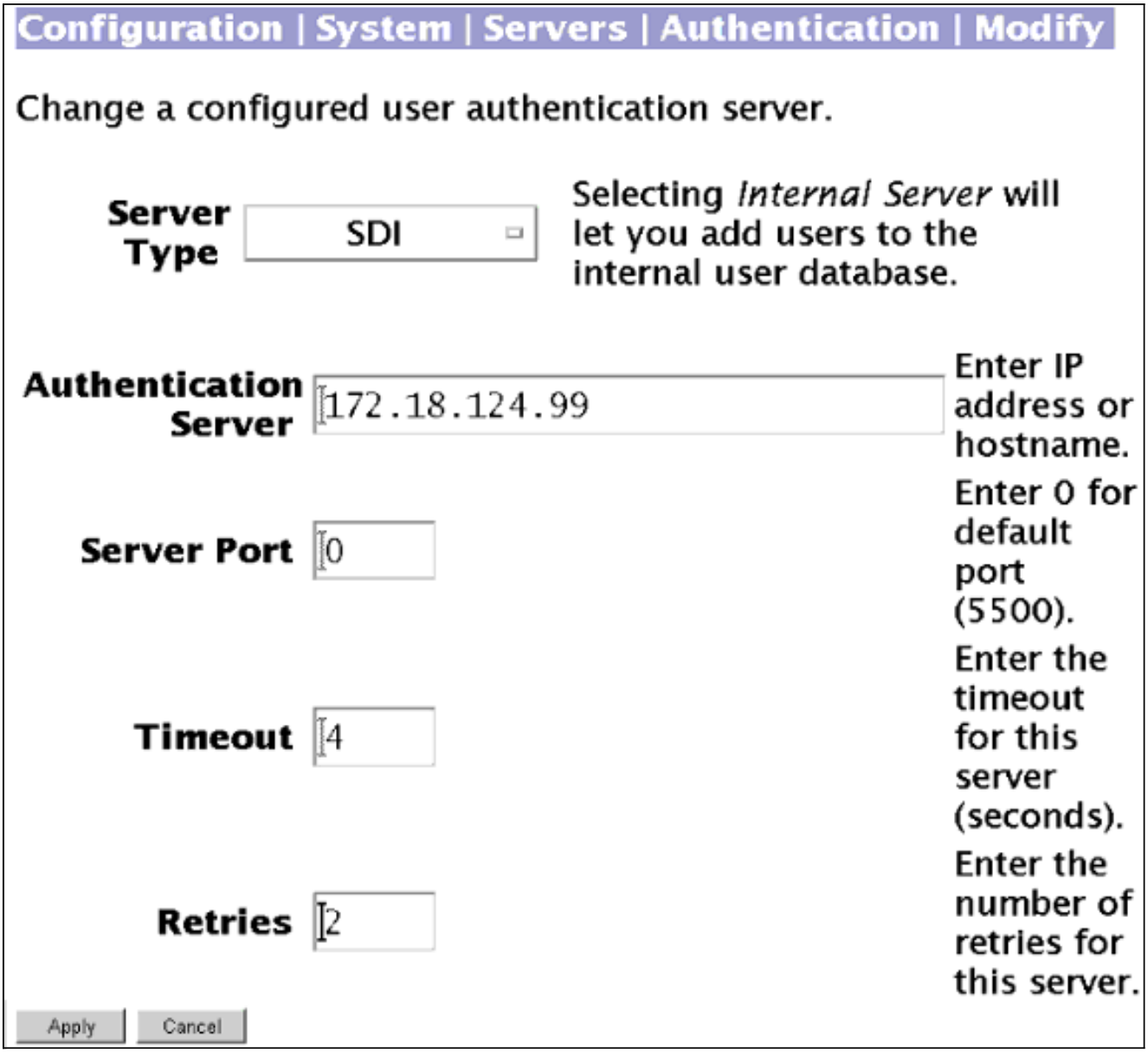
ملاحظة: يعتبر مركز الشبكة الخاصة الظاهرية (VPN) 3000 عميلا لخادم SDI؛ الشاشة التالية هي شاشة عميل إضافة/تحرير خادم SDI. نظرا لأنه عميل جديد، يتم مسح مربع "سر العقدة المرسلة". لم تتح لخادم SDI فرصة إرسال الملف "سر العقدة" إلى مركز التركيز (سيتم عرض هذا الملف في مركز التركيز في **الإدارة > إدارة الملفات** قسم **الملفات** ك "SECURITYid"). بعد مصادقة ناجحة من ال VPN 3000، يعرض الملف "سر العقدة" على ال VPN 3000 Concentrator ويعين ال "Send Node Secret" صندوق.

5. انقر فوق **عمليات تنشيط المستخدم** وتحقق من تضمين المستخدم.

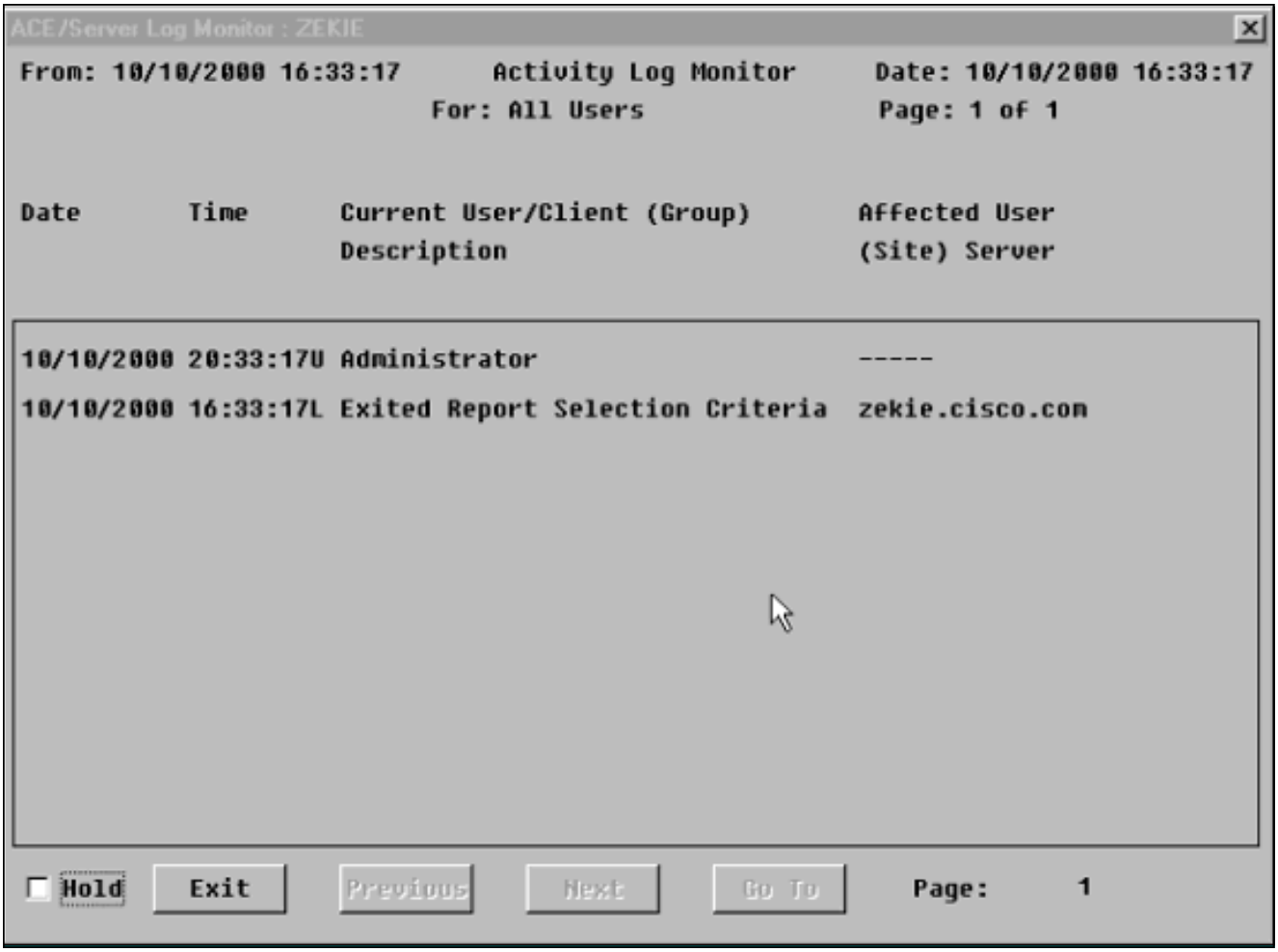
تكوين مركز VPN 3000 واختباره إلى SDI

أستخدم الخطوات التالية لتكوين مركز VPN 3000 واختباره على SDI.

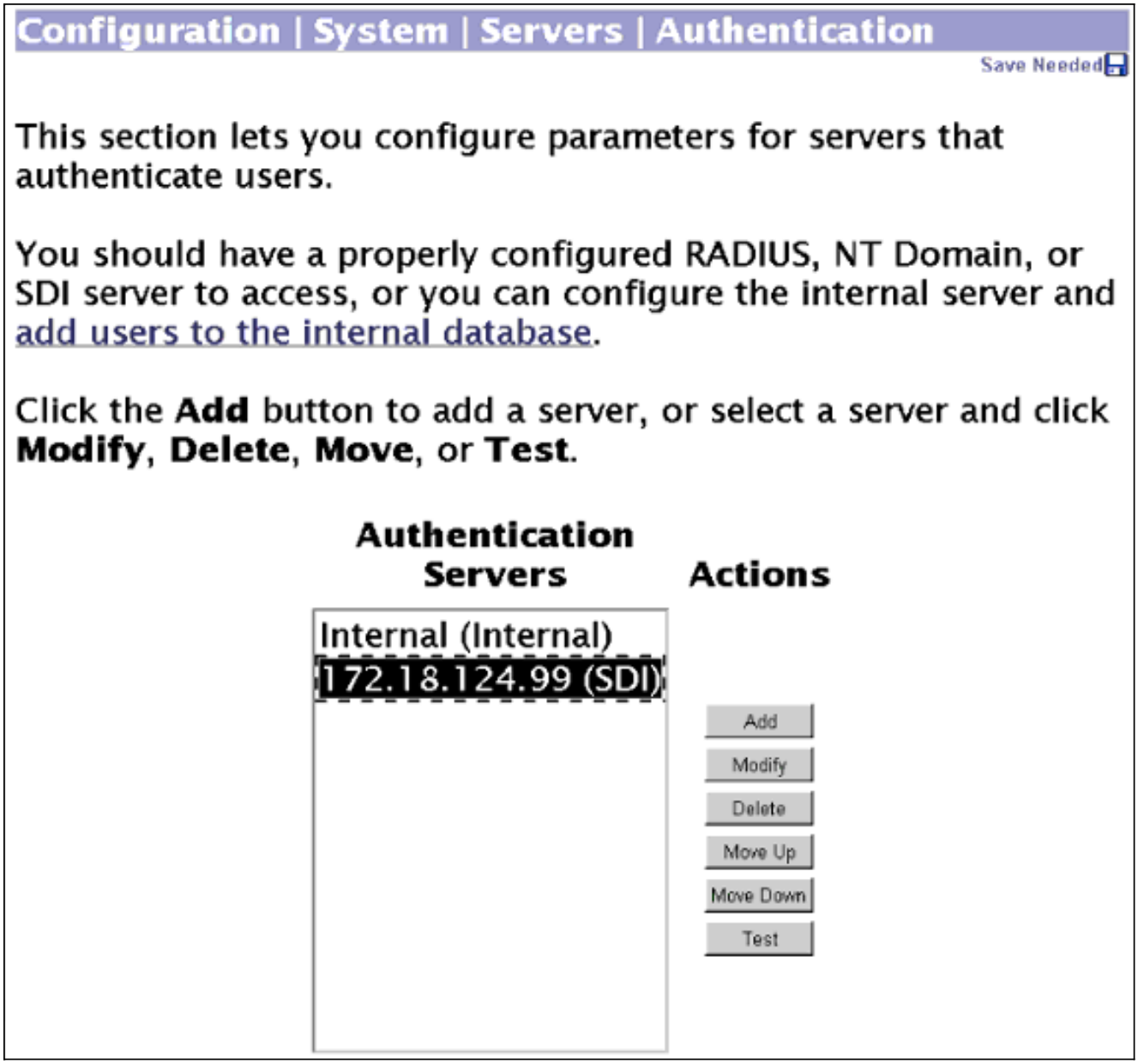
1. أستخدم الشاشة التالية لتكوين مركز VPN 3000 للمصادقة على SDI:



2. من **SDI**، انتقل إلى **التقرير > مراقبة السجل > مراقبة النشاط** وانقر فوق **موافق** لمراقبة الطلبات الواردة.



3. على مركز VPN 3000، انقر على **إختبار** الاتصال.



4. إذا كانت المصادقة جيدة، يعرض مركز VPN 3000:**تمت المصادقة بنجاح**

في المثال أعلاه، قمنا بتعريف خادم SDI عالمي واحد. يمكننا أيضا إختيار تعريف خوادم SDI الفردية لكل مجموعة بالانتقال إلى **التكوين > إدارة المستخدم > المجموعات**، مع إلقاء الضوء على المجموعة المقابلة، واختيار **تعديل خادم المصادقة**.

للحصول على معلومات تصحيح الأخطاء، ارجع إلى الأقسام التالية في هذا المستند:

- تشغيل تصحيح الأخطاء على مركز VPN 3000
- تصحيح أخطاء جيد مع SDI
- تصحيح أخطاء غير صحيح

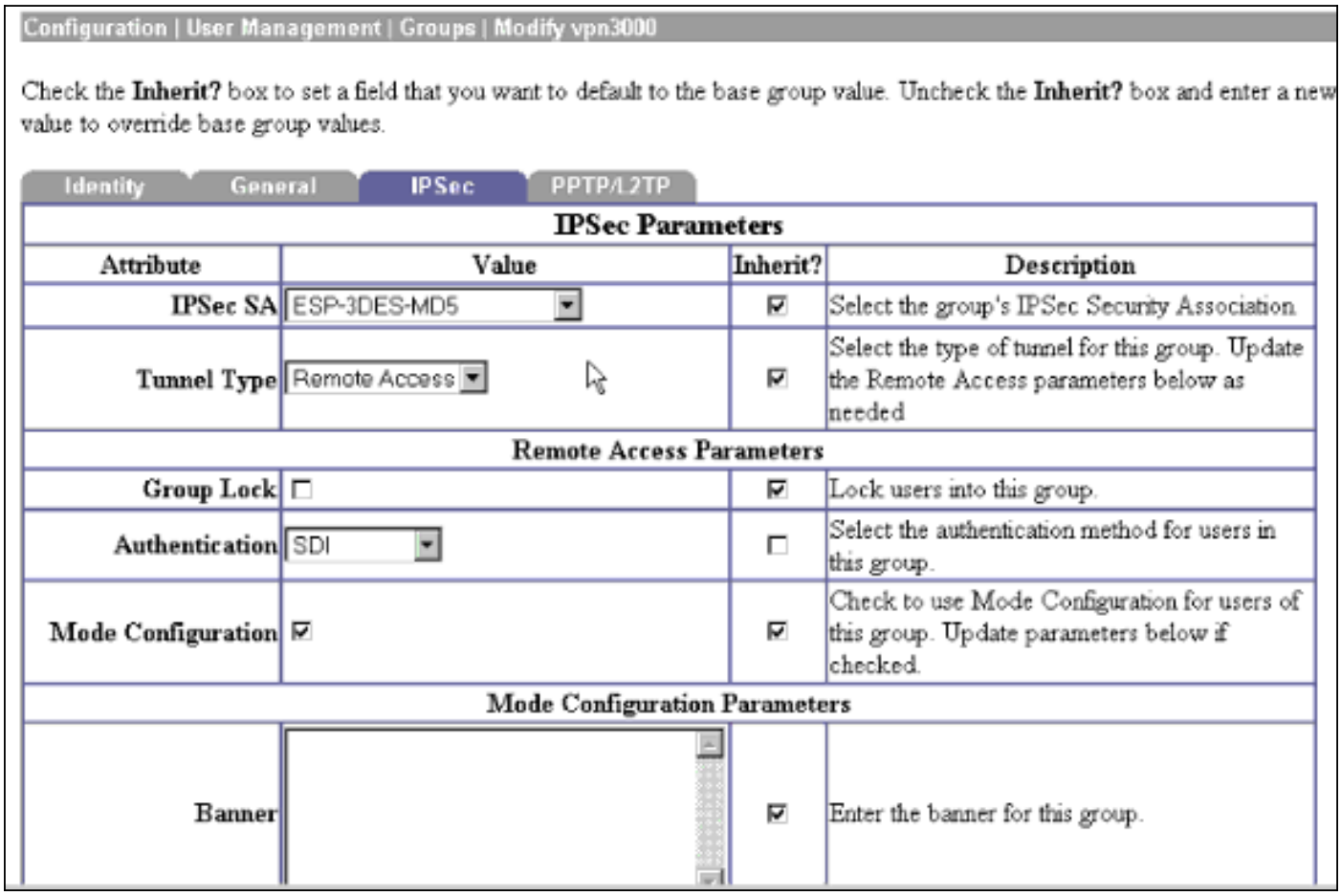
التحقق من الصحة

يوفر هذا القسم معلومات يمكنك إستخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

إختبار عميل Cisco VPN إلى مركز VPN 3000 مع SDI

إذا كان كل شيء يعمل حتى هذه النقطة، فقد حان الوقت لدمج خادم Cisco VPN Client، و VPN 3000 Concentrator، و SDI. نحتاج إلى إجراء تغيير واحد على مركز الشبكة الخاصة الظاهرية (VPN) 3000 من خلال

تعديل مجموعة العمل التي أطلقنا عليها اسم "VPN3000" لإرسال الطلبات إلى خادم SDI.


Configuration | User Management | Groups | Modify vpn3000

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | IPSec | PPTP/L2TP

IPSec Parameters			
Attribute	**Value**	**Inherit?**	**Description**
IPSec SA	ESP-3DES-MD5	☑	Select the group's IPSec Security Association
Tunnel Type	Remote Access	☑	Select the type of tunnel for this group. Update the Remote Access parameters below as needed
Remote Access Parameters			
Group Lock	☐	☑	Lock users into this group.
Authentication	SDI	☐	Select the authentication method for users in this group.
Mode Configuration	☑	☑	Check to use Mode Configuration for users of this group. Update parameters below if checked.
Mode Configuration Parameters			
Banner		☑	Enter the banner for this group.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

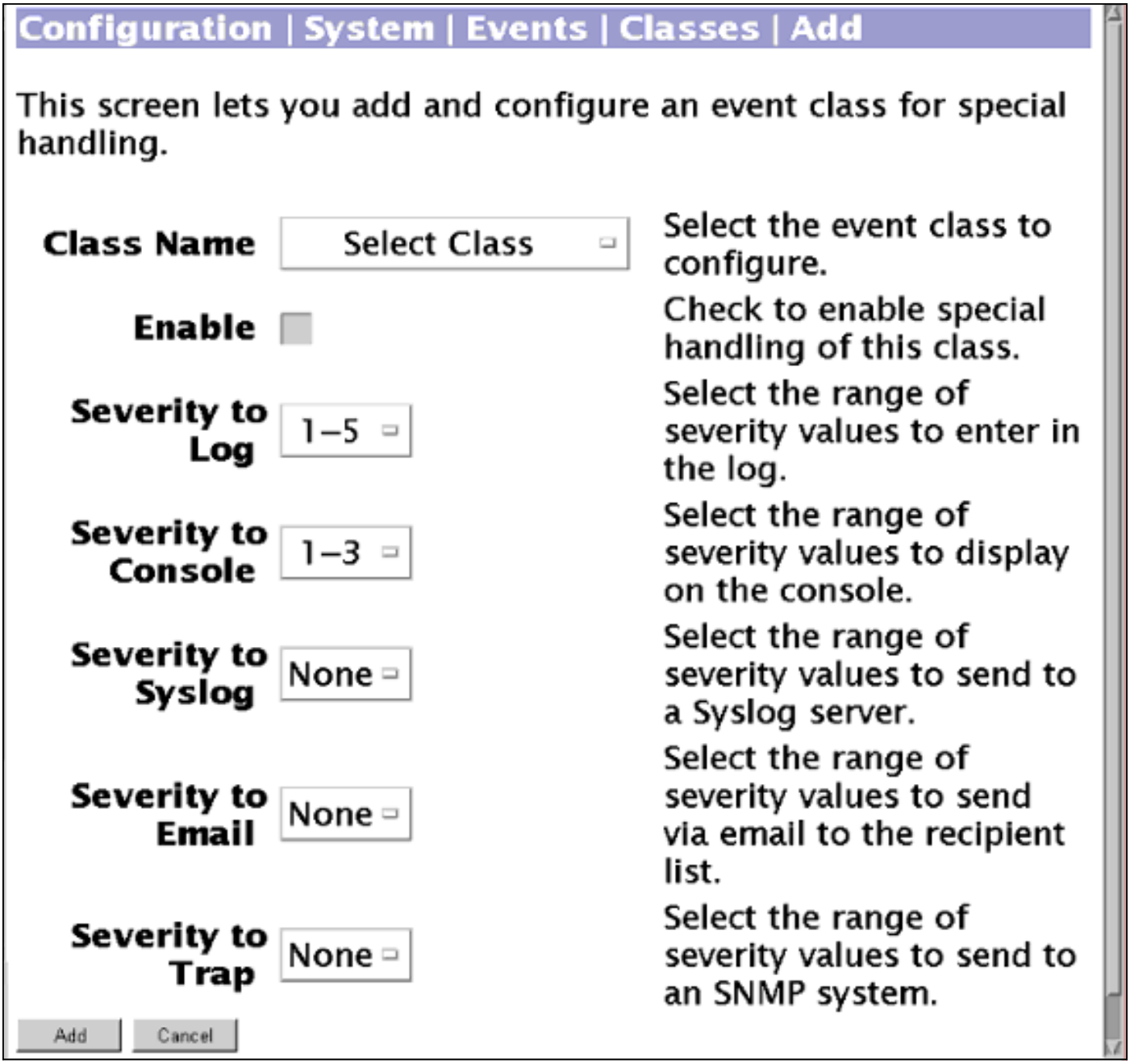
تشغيل تصحيح الأخطاء على مركز VPN 3000

اسم الفئة للمصادقة:

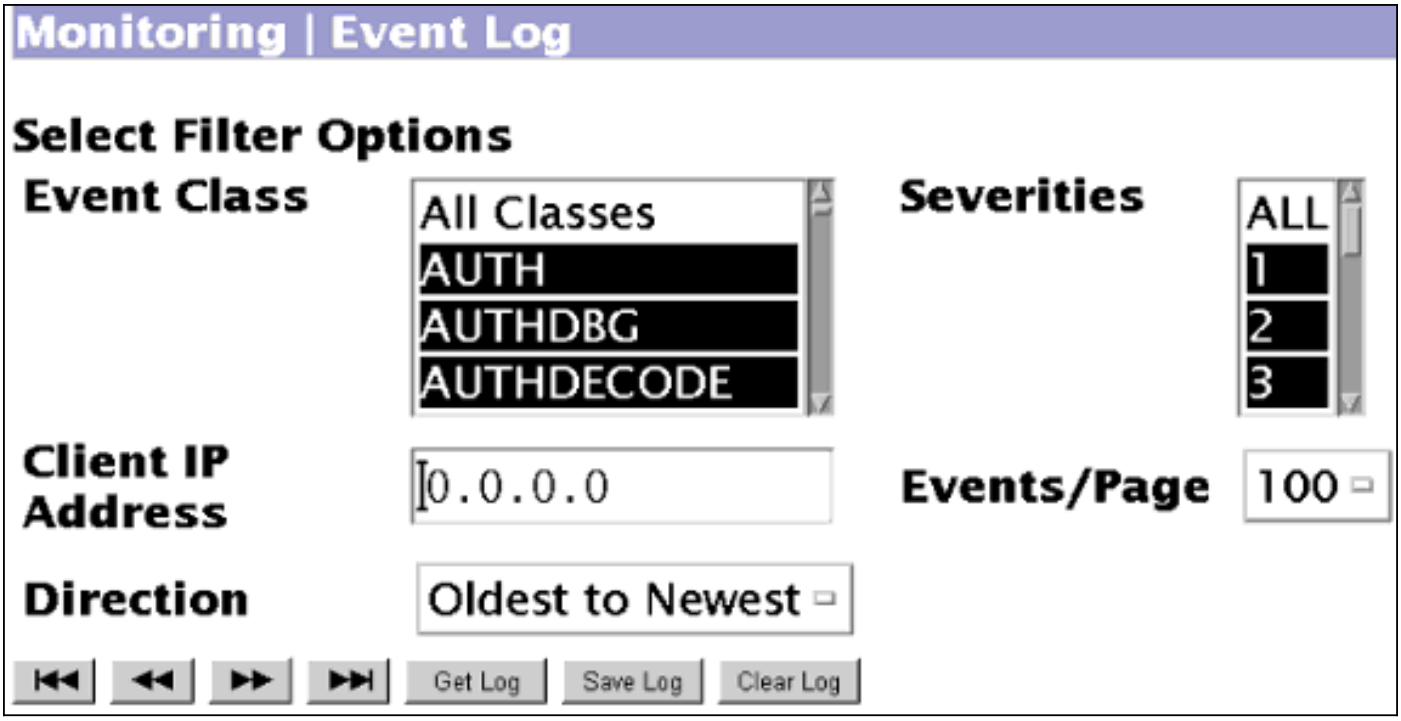
- AUTH
- Authdbg
- أوثديكود

اسم الفئة ل IPSec:

- IKE، IKEDBG، IKEDECODE
- IPSec و IPSECDBG و IPSECDECODE
- الخطورة إلى السجل = 1-9
- الخطورة بالنسبة لوحدة التحكم = 1-3



انقر فوق **الحصول على سجل** لعرض نتائج عملية تصحيح الأخطاء.



تصحيح أخطاء IPSec بشكل جيد باستخدام المصادقة المحلية

```
SEV=8 IKEDECODE/0 RPT=1 161.44.17.135 17:12:32.560 10/10/2000 1
                          ( ISAKMP HEADER :         ( Version 1.0
                Initiator Cookie(8):  9D F3 34 FE 89 BF AA B2
                Responder Cookie(8):  00 00 00 00 00 00 00 00
                                 (Next Payload  :       SA (1
                 Exchange Type :       Oakley Aggressive Mode
                                       Flags          :       0
                                       Message ID     :       0
                                     Length         :       307

          SEV=8 IKEDBG/0 RPT=1 161.44.17.135 17:12:32.560 10/10/2000 7
                                  : RECEIVED Message (msgid=0) with payloads
(HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + VENDOR (13) + NONE (0
                                                 total length : 307 ...

            SEV=9 IKEDBG/0 RPT=2 161.44.17.135 17:12:32.560 10/10/2000 10
                                                  processing SA payload

       SEV=8 IKEDECODE/0 RPT=2 161.44.17.135 17:12:32.560 10/10/2000 11
                                                  : SA Payload Decode
                                       (DOI           :       IPSEC (1
                                 (Situation     :       Identity Only (1
                                     Length         :       120

       SEV=8 IKEDECODE/0 RPT=3 161.44.17.135 17:12:32.560 10/10/2000 14
                                                    :Proposal Decode
                                         Proposal #     :       1
                                  (Protocol ID   :       ISAKMP (1
                                         of Transforms:       4#
                                Spi             :       00 00 00 00
                                       Length         :       108

       SEV=8 IKEDECODE/0 RPT=4 161.44.17.135 17:12:32.560 10/10/2000 18
                                  :Transform # 1 Decode for Proposal # 1
                                         Transform #    :       1
                                   (Transform ID  :       IKE (1
```

```
                                        Length        :       24

SEV=8 IKEDECODE/0 RPT=5 161.44.17.135 17:12:32.560 10/10/2000 20
                    :Phase 1 SA Attribute Decode for Transform # 1
                              (Encryption Alg:       DES-CBC (1
                                  (Hash Alg      :       MD5 (1
                             (DH Group      :       Oakley Group 1 (1
                              (Auth Method   :       Preshared Key (1

SEV=8 IKEDECODE/0 RPT=6 161.44.17.135 17:12:32.560 10/10/2000 24
                             :Transform # 2 Decode for Proposal # 1
                                          Transform #   :       2
                                    (Transform ID  :       IKE (1
                                         Length        :       24

SEV=8 IKEDECODE/0 RPT=7 161.44.17.135 17:12:32.560 10/10/2000 26
                    :Phase 1 SA Attribute Decode for Transform # 2
                              (Encryption Alg:       Triple-DES (5
                                  (Hash Alg      :       MD5 (1
                             (DH Group      :       Oakley Group 1 (1
                              (Auth Method   :       Preshared Key (1

SEV=8 IKEDECODE/0 RPT=8 161.44.17.135 17:12:32.560 10/10/2000 30
                             :Transform # 3 Decode for Proposal # 1
                                          Transform #   :       3
                                    (Transform ID  :       IKE (1
                                         Length        :       24

SEV=8 IKEDECODE/0 RPT=9 161.44.17.135 17:12:32.560 10/10/2000 32
                    :Phase 1 SA Attribute Decode for Transform # 3
                              (Encryption Alg:       Triple-DES (5
                                  (Hash Alg      :       SHA (2
                             (DH Group      :       Oakley Group 1 (1
                              (Auth Method   :       Preshared Key (1

SEV=8 IKEDECODE/0 RPT=10 161.44.17.135 17:12:32.560 10/10/2000 36
                             :Transform # 4 Decode for Proposal # 1
                                          Transform #   :       4
                                    (Transform ID  :       IKE (1
                                         Length        :       24

SEV=8 IKEDECODE/0 RPT=11 161.44.17.135 17:12:32.560 10/10/2000 38
                    :Phase 1 SA Attribute Decode for Transform # 4
                              (Encryption Alg:       DES-CBC (1
                                  (Hash Alg      :       SHA (2
                             (DH Group      :       Oakley Group 1 (1
                              (Auth Method   :       Preshared Key (1

   SEV=8 IKEDBG/0 RPT=3 161.44.17.135 17:12:32.560 10/10/2000 42
                 Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
                                      :Parsing received transform
               :Phase 1 failure against global IKE proposal # 1
                     :Mismatched attr types for class DH Group
                                       Rcv'd: Oakley Group 1
                                       Cfg'd: Oakley Group 2

   SEV=8 IKEDBG/0 RPT=4 161.44.17.135 17:12:32.560 10/10/2000 47
               :Phase 1 failure against global IKE proposal # 2
                :Mismatched attr types for class Encryption Alg
                                            Rcv'd: DES-CBC
                                        Cfg'd: Triple-DES

   SEV=8 IKEDBG/0 RPT=5 161.44.17.135 17:12:32.560 10/10/2000 50
                 Proposal # 1, Transform # 2, Type ISAKMP, Id IKE
```

```
                                    :Parsing received transform
            :Phase 1 failure against global IKE proposal # 1
                   :Mismatched attr types for class DH Group
                                      Rcv'd: Oakley Group 1
                                      Cfg'd: Oakley Group 2

 SEV=8 IKEDBG/0 RPT=6 161.44.17.135 17:12:32.560 10/10/2000 55
              Proposal # 1, Transform # 3, Type ISAKMP, Id IKE
                                    :Parsing received transform
            :Phase 1 failure against global IKE proposal # 1
                   :Mismatched attr types for class DH Group
                                      Rcv'd: Oakley Group 1
                                      Cfg'd: Oakley Group 2

 SEV=8 IKEDBG/0 RPT=7 161.44.17.135 17:12:32.560 10/10/2000 60
            :Phase 1 failure against global IKE proposal # 2
                   :Mismatched attr types for class Hash Alg
                                                Rcv'd: SHA
                                                Cfg'd: MD5

 SEV=8 IKEDBG/0 RPT=8 161.44.17.135 17:12:32.560 10/10/2000 62
            :Phase 1 failure against global IKE proposal # 3
             :Mismatched attr types for class Encryption Alg
                                           Rcv'd: Triple-DES
                                              Cfg'd: DES-CBC

 SEV=8 IKEDBG/0 RPT=9 161.44.17.135 17:12:32.560 10/10/2000 65
              Proposal # 1, Transform # 4, Type ISAKMP, Id IKE
                                    :Parsing received transform
            :Phase 1 failure against global IKE proposal # 1
                   :Mismatched attr types for class DH Group
                                      Rcv'd: Oakley Group 1
                                      Cfg'd: Oakley Group 2

SEV=8 IKEDBG/0 RPT=10 161.44.17.135 17:12:32.560 10/10/2000 70
            :Phase 1 failure against global IKE proposal # 2
             :Mismatched attr types for class Encryption Alg
                                                Rcv'd: DES-CBC
                                           Cfg'd: Triple-DES

SEV=8 IKEDBG/0 RPT=11 161.44.17.135 17:12:32.560 10/10/2000 73
            :Phase 1 failure against global IKE proposal # 3
                   :Mismatched attr types for class Hash Alg
                                                Rcv'd: SHA
                                                Cfg'd: MD5

SEV=7 IKEDBG/0 RPT=12 161.44.17.135 17:12:32.560 10/10/2000 75
                                    Oakley proposal is acceptable

SEV=9 IKEDBG/0 RPT=13 161.44.17.135 17:12:32.560 10/10/2000 76
                                           processing ke payload

SEV=9 IKEDBG/0 RPT=14 161.44.17.135 17:12:32.560 10/10/2000 77
                                             processing ISA_KE

 SEV=9 IKEDBG/1 RPT=1 161.44.17.135 17:12:32.560 10/10/2000 78
                                          processing nonce payload

 SEV=9 IKEDBG/1 RPT=2 161.44.17.135 17:12:32.560 10/10/2000 79
                                               Processing ID

 SEV=9 IKEDBG/1 RPT=3 161.44.17.135 17:12:32.560 10/10/2000 80
                                          processing vid payload
```

```
SEV=9 IKEDBG/23 RPT=1 161.44.17.135 17:12:32.580 10/10/2000 81
                  Starting group lookup for peer 161.44.17.135

SEV=7 IKEDBG/0 RPT=15 161.44.17.135 17:12:32.680 10/10/2000 82
                                  (Found Phase 1 Group (vpn3000

SEV=7 IKEDBG/14 RPT=1 161.44.17.135 17:12:32.680 10/10/2000 83
                          Authentication configured for Internal

SEV=9 IKEDBG/0 RPT=16 161.44.17.135 17:12:32.680 10/10/2000 84
                                    constructing ISA_SA for isakmp

SEV=9 IKEDBG/0 RPT=17 161.44.17.135 17:12:32.680 10/10/2000 85
                                          constructing ke payload

 SEV=9 IKEDBG/1 RPT=4 161.44.17.135 17:12:32.680 10/10/2000 86
                                        constructing nonce payload

    SEV=9 IKE/0 RPT=1 161.44.17.135 17:12:32.680 10/10/2000 87
                                  ...Generating keys for Responder

 SEV=9 IKEDBG/1 RPT=5 161.44.17.135 17:12:32.680 10/10/2000 88
                                                 constructing ID

              SEV=9 IKEDBG/0 RPT=18 17:12:32.680 10/10/2000 89
                                          construct hash payload

SEV=9 IKEDBG/0 RPT=19 161.44.17.135 17:12:32.680 10/10/2000 90
                                                  computing hash

 SEV=9 IKEDBG/1 RPT=6 161.44.17.135 17:12:32.680 10/10/2000 91
                                        constructing vid payload

SEV=8 IKEDBG/0 RPT=20 161.44.17.135 17:12:32.680 10/10/2000 92
                       : SENDING Message (msgid=0) with payloads
                            HDR + SA (1)  ... total length : 248

SEV=8 IKEDECODE/0 RPT=12 161.44.17.135 17:12:32.730 10/10/2000 93
                               ( ISAKMP HEADER :         ( Version 1.0
                    Initiator Cookie(8):  9D F3 34 FE 89 BF AA B2
                    Responder Cookie(8):  B7 AD 34 D2 74 4D 05 DA
                                  (Next Payload  :       HASH (8
                     Exchange Type :       Oakley Aggressive Mode
                             ( Flags         :       1   (ENCRYPT
                                          Message ID    :       0
                                         Length        :       52

SEV=8 IKEDBG/0 RPT=21 161.44.17.135 17:12:32.730 10/10/2000 99
                       : RECEIVED Message (msgid=0) with payloads
                    HDR + HASH (8) + NONE (0) ... total length : 48

  SEV=9 IKEDBG/0 RPT=22 161.44.17.135 17:12:32.730 10/10/2000 101
                                                 processing hash

  SEV=9 IKEDBG/0 RPT=23 161.44.17.135 17:12:32.730 10/10/2000 102
                                                  computing hash

SEV=8 IKEDECODE/0 RPT=13 161.44.17.135 17:12:33.410 10/10/2000 103
                               ( ISAKMP HEADER :         ( Version 1.0
                    Initiator Cookie(8):  9D F3 34 FE 89 BF AA B2
                    Responder Cookie(8):  B7 AD 34 D2 74 4D 05 DA
                                  (Next Payload  :       HASH (8
                          Exchange Type :       Oakley Quick Mode
                             ( Flags         :       1   (ENCRYPT
```

```
                                        Message ID    :       48687ca1
                                             Length        :       308

                    SEV=9 IKEDBG/21 RPT=1 161.44.17.135 17:12:33.410 10/10/2000 110
                  Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress

                    SEV=9 IKEDBG/0 RPT=24 161.44.17.135 17:12:33.410 10/10/2000 111
                                                  constructing blank hash

                    SEV=9 IKEDBG/0 RPT=25 161.44.17.135 17:12:33.410 10/10/2000 112
                                                    constructing qm hash

                    SEV=8 IKEDBG/0 RPT=26 161.44.17.135 17:12:33.410 10/10/2000 113
                                  : SENDING Message (msgid=fc2ce5eb) with payloads
                                             HDR + HASH (8)  ... total length : 68

                SEV=8 IKEDECODE/0 RPT=14 161.44.17.135 17:12:44.680 10/10/2000 115
                                          ( ISAKMP HEADER :         ( Version 1.0
                                   Initiator Cookie(8):  9D F3 34 FE 89 BF AA B2
                                   Responder Cookie(8):  B7 AD 34 D2 74 4D 05 DA
                                                (Next Payload  :       HASH (8
                                      Exchange Type :       Oakley Transactional
                                            ( Flags         :       1   (ENCRYPT
                                                  Message ID    :       fc2ce5eb
                                                       Length        :       92

                    SEV=8 IKEDBG/0 RPT=27 161.44.17.135 17:12:44.680 10/10/2000 122
                                 : RECEIVED Message (msgid=fc2ce5eb) with payloads
                      HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 85

                                   SEV=9 IKEDBG/1 RPT=7 17:12:44.680 10/10/2000 124
                                                    !process_attr(): Enter

                                   SEV=9 IKEDBG/1 RPT=8 17:12:44.680 10/10/2000 125
                                                  .Processing cfg reply attributes

                    SEV=7 IKEDBG/14 RPT=2 161.44.17.135 17:12:44.980 10/10/2000 126
                                                          [ User [ 37297304
                                       Authentication configured for Internal

                       SEV=4 IKE/52 RPT=7 161.44.17.135 17:12:44.980 10/10/2000 127
                                                          [ User [ 37297304
                                                .User (37297304) authenticated

                    SEV=9 IKEDBG/31 RPT=1 161.44.17.135 17:12:44.980 10/10/2000 128
                                                          [ User [ 37297304
(Obtained IP addr (192.168.1.1) prior to initiating Mode Cfg (XAuth enabled

                    SEV=9 IKEDBG/0 RPT=28 161.44.17.135 17:12:44.980 10/10/2000 130
                                                          [ User [ 37297304
                                                  constructing blank hash

                    SEV=9 IKEDBG/0 RPT=29 161.44.17.135 17:12:44.980 10/10/2000 131
                      ............                C0A80101 F0010000 00010004 :0000

                    SEV=9 IKEDBG/0 RPT=30 161.44.17.135 17:12:44.980 10/10/2000 132
                                                          [ User [ 37297304
                                                    constructing QM hash

                    SEV=8 IKEDBG/0 RPT=31 161.44.17.135 17:12:44.980 10/10/2000 133
                                  : SENDING Message (msgid=fc2ce5eb) with payloads
                                             HDR + HASH (8)  ... total length : 80

                SEV=8 IKEDECODE/0 RPT=15 161.44.17.135 17:12:44.990 10/10/2000 135
```

```
                                        ( ISAKMP HEADER :         ( Version 1.0
                                  Initiator Cookie(8):  9D F3 34 FE 89 BF AA B2
                                  Responder Cookie(8):  B7 AD 34 D2 74 4D 05 DA
                                                (Next Payload  :       HASH (8
                                     Exchange Type :       Oakley Transactional
                                           ( Flags         :       1   (ENCRYPT
                                                Message ID    :       fc2ce5eb
                                                      Length        :       68

                        SEV=8 IKEDBG/0 RPT=32 161.44.17.135 17:12:44.990 10/10/2000 142
                                      : RECEIVED Message (msgid=fc2ce5eb) with payloads
                            HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 64

                                       SEV=9 IKEDBG/1 RPT=9 17:12:44.990 10/10/2000 144
                                                            !process_attr(): Enter

                                      SEV=9 IKEDBG/1 RPT=10 17:12:44.990 10/10/2000 145
                                                    Processing cfg ACK attributes

                                      SEV=9 IKEDBG/1 RPT=11 17:12:44.990 10/10/2000 146
                                                    !Received IPV4 address ack

                                      SEV=9 IKEDBG/1 RPT=12 17:12:44.990 10/10/2000 147
                                                         !Received Save PW ack

                                       SEV=4 AUTH/21 RPT=18 17:12:44.990 10/10/2000 148
                                                       User 37297304 connected

                        SEV=7 IKEDBG/22 RPT=1 161.44.17.135 17:12:44.990 10/10/2000 149
                                                                [ User [ 37297304
                        Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed

                        SEV=8 IKEDBG/0 RPT=33 161.44.17.135 17:12:44.990 10/10/2000 151
                                      : RECEIVED Message (msgid=48687ca1) with payloads
(HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0
                                                       total length : 304 ...

                        SEV=9 IKEDBG/0 RPT=34 161.44.17.135 17:12:44.990 10/10/2000 154
                                                                [ User [ 37297304
                                                                  processing hash

                        SEV=9 IKEDBG/0 RPT=35 161.44.17.135 17:12:44.990 10/10/2000 155
                                                                [ User [ 37297304
                                                             processing SA payload

                     SEV=8 IKEDECODE/0 RPT=16 161.44.17.135 17:12:44.990 10/10/2000 156
                                                               : SA Payload Decode
                                                  (DOI           :       IPSEC (1
                                              (Situation     :       Identity Only (1
                                                           Length        :       180

                     SEV=8 IKEDECODE/0 RPT=17 161.44.17.135 17:12:44.990 10/10/2000 159
                                                                 :Proposal Decode
                                                       Proposal #    :       1
                                                (Protocol ID   :       ESP (3
                                                      of Transforms:       1#
                                                Spi           :       99 15 18 B4
                                                      Length        :       28

                     SEV=8 IKEDECODE/0 RPT=18 161.44.17.135 17:12:44.990 10/10/2000 163
                                                :Transform # 1 Decode for Proposal # 1
                                                      Transform #   :       1
                                                (Transform ID  :       DES-CBC (2
                                                      Length        :       16
```

```
SEV=8 IKEDECODE/0 RPT=19 161.44.17.135 17:12:44.990 10/10/2000 165
                    :Phase 2 SA Attribute Decode for Transform # 1
                                 (HMAC Algorithm:       MD5 (1
                               (Encapsulation :       Tunnel (1

SEV=8 IKEDECODE/0 RPT=20 161.44.17.135 17:12:44.990 10/10/2000 167
                                                  :Proposal Decode
                                       Proposal #    :       2
                                  (Protocol ID   :       ESP (3
                                       of Transforms:       1#
                             Spi           :       99 15 18 B4
                                     Length        :       28

SEV=8 IKEDECODE/0 RPT=21 161.44.17.135 17:12:44.990 10/10/2000 171
                           :Transform # 1 Decode for Proposal # 2
                                       Transform #   :       1
                           (Transform ID  :       Triple-DES (3
                                     Length        :       16

SEV=8 IKEDECODE/0 RPT=22 161.44.17.135 17:12:44.990 10/10/2000 173
                    :Phase 2 SA Attribute Decode for Transform # 1
                                 (HMAC Algorithm:       MD5 (1
                               (Encapsulation :       Tunnel (1

SEV=8 IKEDECODE/0 RPT=23 161.44.17.135 17:12:44.990 10/10/2000 175
                                                  :Proposal Decode
                                       Proposal #    :       3
                                  (Protocol ID   :       ESP (3
                                       of Transforms:       1#
                             Spi           :       99 15 18 B4
                                     Length        :       28

SEV=8 IKEDECODE/0 RPT=24 161.44.17.135 17:12:44.990 10/10/2000 179
                           :Transform # 1 Decode for Proposal # 3
                                       Transform #   :       1
                              (Transform ID  :       DES-CBC (2
                                     Length        :       16

SEV=8 IKEDECODE/0 RPT=25 161.44.17.135 17:12:44.990 10/10/2000 181
                    :Phase 2 SA Attribute Decode for Transform # 1
                                 (HMAC Algorithm:       SHA (2
                               (Encapsulation :       Tunnel (1

SEV=8 IKEDECODE/0 RPT=26 161.44.17.135 17:12:44.990 10/10/2000 183
                                                  :Proposal Decode
                                       Proposal #    :       4
                                  (Protocol ID   :       ESP (3
                                       of Transforms:       1#
                             Spi           :       99 15 18 B4
                                     Length        :       28

SEV=8 IKEDECODE/0 RPT=27 161.44.17.135 17:12:44.990 10/10/2000 187
                           :Transform # 1 Decode for Proposal # 4
                                       Transform #   :       1
                           (Transform ID  :       Triple-DES (3
                                     Length        :       16

SEV=8 IKEDECODE/0 RPT=28 161.44.17.135 17:12:44.990 10/10/2000 189
                    :Phase 2 SA Attribute Decode for Transform # 1
                                 (HMAC Algorithm:       SHA (2
                               (Encapsulation :       Tunnel (1

SEV=8 IKEDECODE/0 RPT=29 161.44.17.135 17:12:44.990 10/10/2000 191
```

```
                                                    :Proposal Decode
                                                Proposal #    :       5
                                            (Protocol ID   :       ESP (3
                                                  of Transforms:       1#
                                        Spi           :       99 15 18 B4
                                                Length        :       28

SEV=8 IKEDECODE/0 RPT=30 161.44.17.135 17:12:44.990 10/10/2000 195
                                  :Transform # 1 Decode for Proposal # 5
                                              Transform #   :       1
                                     (Transform ID  :       NULL (11
                                              Length        :       16

SEV=8 IKEDECODE/0 RPT=31 161.44.17.135 17:12:44.990 10/10/2000 197
                          :Phase 2 SA Attribute Decode for Transform # 1
                                       (HMAC Algorithm:       MD5 (1
                                    (Encapsulation :       Tunnel (1

SEV=8 IKEDECODE/0 RPT=32 161.44.17.135 17:12:44.990 10/10/2000 199
                                                    :Proposal Decode
                                                Proposal #    :       6
                                            (Protocol ID   :       ESP (3
                                                  of Transforms:       1#
                                        Spi           :       99 15 18 B4
                                                Length        :       28

SEV=8 IKEDECODE/0 RPT=33 161.44.17.135 17:12:44.990 10/10/2000 203
                                  :Transform # 1 Decode for Proposal # 6
                                              Transform #   :       1
                                     (Transform ID  :       NULL (11
                                              Length        :       16

SEV=8 IKEDECODE/0 RPT=34 161.44.17.135 17:12:44.990 10/10/2000 205
                          :Phase 2 SA Attribute Decode for Transform # 1
                                       (HMAC Algorithm:       SHA (2
                                    (Encapsulation :       Tunnel (1

   SEV=9 IKEDBG/1 RPT=13 161.44.17.135 17:12:44.990 10/10/2000 207
                                                    [ User [ 37297304
                                          processing nonce payload

   SEV=9 IKEDBG/1 RPT=14 161.44.17.135 17:12:44.990 10/10/2000 208
                                                    [ User [ 37297304
                                                        Processing ID

     SEV=5 IKE/25 RPT=13 161.44.17.135 17:12:44.990 10/10/2000 209
                                                    [ User [ 37297304
                          :Received remote Proxy Host data in ID Payload
                               Address 161.44.17.135, Protocol 0, Port 0

   SEV=7 IKEDBG/1 RPT=15 161.44.17.135 17:12:44.990 10/10/2000 212
                                                    [ User [ 37297304
                                     !Modifying client proxy src address

   SEV=9 IKEDBG/1 RPT=16 161.44.17.135 17:12:44.990 10/10/2000 213
                                                    [ User [ 37297304
                                                        Processing ID

      SEV=5 IKE/24 RPT=7 161.44.17.135 17:12:44.990 10/10/2000 214
                                                    [ User [ 37297304
                           :Received local Proxy Host data in ID Payload
                              Address 172.18.124.134, Protocol 0, Port 0

   SEV=9 IKEDBG/0 RPT=36 161.44.17.135 17:12:44.990 10/10/2000 217
```

```
                                                                  [ User [ 37297304
                                                    Processing Notify payload

          SEV=8 IKEDECODE/0 RPT=35 161.44.17.135 17:12:44.990 10/10/2000 218
                                                    : Notify Payload Decode
                                                (DOI           :       IPSEC (1
                                               (Protocol       :       ISAKMP (1
                                  (Message       :       Initial contact (24578
     Spi           :       9D F3 34 FE 89 BF AA B2 B7 AD 34 D2 74 4D 05 DA
                                                Length         :       28

                                SEV=8 IKEDBG/0 RPT=37 17:12:44.990 10/10/2000 224
                                            QM IsRekeyed old sa not found by addr

                    SEV=5 IKE/66 RPT=13 161.44.17.135 17:12:44.990 10/10/2000 225
                                                                  [ User [ 37297304
                                  IKE Remote Peer configured for SA: ESP-3DES-MD5

                   SEV=9 IKEDBG/0 RPT=38 161.44.17.135 17:12:44.990 10/10/2000 226
                                                                  [ User [ 37297304
                                                               processing IPSEC SA

                                SEV=8 IKEDBG/0 RPT=39 17:12:44.990 10/10/2000 227
                                Proposal # 1, Transform # 1, Type ESP, Id DES-CBC
                                                    :Parsing received transform
                                                             :Phase 2 failure
                                        :Mismatched transform IDs for protocol ESP
                                                               Rcv'd: DES-CBC
                                                            Cfg'd: Triple-DES

                   SEV=7 IKEDBG/27 RPT=1 161.44.17.135 17:12:45.000 10/10/2000 232
                                                                  [ User [ 37297304
                                  IPSec SA Proposal # 2, Transform # 1 acceptable

                   SEV=7 IKEDBG/0 RPT=40 161.44.17.135 17:12:45.000 10/10/2000 233
                                                                  [ User [ 37297304
                                                             !IKE: requesting SPI

                                   SEV=6 IKE/0 RPT=2 17:12:45.000 10/10/2000 234
          AM received unexpected event EV_ACTIVATE_NEW_SA in state AM_ACTIVE

                                SEV=9 IPSECDBG/6 RPT=1 17:12:45.000 10/10/2000 235
 ,IPSEC key message parse - msgtype 6, len 164, vers 1, pid 00000000, seq 13
,err 0, type 2, mode 0, state 32, label 0, pad 0, spi 00000000, encrKeyLen 0
         ,hashKeyLen 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 300
                                                  lifetime2 2000000000, dsId 2

                                SEV=9 IPSECDBG/1 RPT=1 17:12:45.000 10/10/2000 239
                                                   !Processing KEY_GETSPI msg

                               SEV=7 IPSECDBG/13 RPT=1 17:12:45.000 10/10/2000 240
                                                      Reserved SPI 1773955517

                                  SEV=8 IKEDBG/6 RPT=1 17:12:45.000 10/10/2000 241
                                     IKE got SPI from key engine: SPI = 0x69bc69bd

                   SEV=9 IKEDBG/0 RPT=41 161.44.17.135 17:12:45.000 10/10/2000 242
                                                                  [ User [ 37297304
                                               oakley constructing quick mode

                   SEV=9 IKEDBG/0 RPT=42 161.44.17.135 17:12:45.000 10/10/2000 243
                                                                  [ User [ 37297304
                                                      constructing blank hash
```

```
SEV=9 IKEDBG/0 RPT=43 161.44.17.135 17:12:45.000 10/10/2000 244
                                                  [ User [ 37297304
                                      constructing ISA_SA for ipsec

SEV=9 IKEDBG/1 RPT=17 161.44.17.135 17:12:45.000 10/10/2000 245
                                                  [ User [ 37297304
                                  constructing ipsec nonce payload

SEV=9 IKEDBG/1 RPT=18 161.44.17.135 17:12:45.000 10/10/2000 246
                                                  [ User [ 37297304
                                               constructing proxy ID

SEV=7 IKEDBG/0 RPT=44 161.44.17.135 17:12:45.000 10/10/2000 247
                                                  [ User [ 37297304
                                             :Transmitting Proxy Id
                    Remote host: 192.168.1.1  Protocol 0  Port 0
                 Local host:  172.18.124.134  Protocol 0  Port 0

SEV=9 IKEDBG/0 RPT=45 161.44.17.135 17:12:45.000 10/10/2000 251
                                                  [ User [ 37297304
                                              constructing QM hash

SEV=8 IKEDBG/0 RPT=46 161.44.17.135 17:12:45.000 10/10/2000 252
                 : SENDING Message (msgid=48687ca1) with payloads
                           HDR + HASH (8)  ... total length : 136

SEV=8 IKEDECODE/0 RPT=36 161.44.17.135 17:12:45.010 10/10/2000 254
                            ( ISAKMP HEADER :         ( Version 1.0
                  Initiator Cookie(8):  9D F3 34 FE 89 BF AA B2
                  Responder Cookie(8):  B7 AD 34 D2 74 4D 05 DA
                                  (Next Payload  :       HASH (8
                        Exchange Type :       Oakley Quick Mode
                           ( Flags         :       1   (ENCRYPT
                                 Message ID    :       48687ca1
                                       Length        :       52

SEV=8 IKEDBG/0 RPT=47 161.44.17.135 17:12:45.010 10/10/2000 261
                : RECEIVED Message (msgid=48687ca1) with payloads
                  HDR + HASH (8) + NONE (0) ... total length : 48

SEV=9 IKEDBG/0 RPT=48 161.44.17.135 17:12:45.010 10/10/2000 263
                                                  [ User [ 37297304
                                                    processing hash

SEV=9 IKEDBG/0 RPT=49 161.44.17.135 17:12:45.010 10/10/2000 264
                                                  [ User [ 37297304
                                               loading all IPSEC SAs

SEV=9 IKEDBG/1 RPT=19 161.44.17.135 17:12:45.010 10/10/2000 265
                                                  [ User [ 37297304
                                          !Generating Quick Mode Key

SEV=9 IKEDBG/1 RPT=20 161.44.17.135 17:12:45.010 10/10/2000 266
                                                  [ User [ 37297304
                                          !Generating Quick Mode Key

SEV=7 IKEDBG/0 RPT=50 161.44.17.135 17:12:45.020 10/10/2000 267
                                                  [ User [ 37297304
                                                      :Loading host
                                             Dst: 172.18.124.134
                                                Src: 192.168.1.1

  SEV=4 IKE/49 RPT=13 161.44.17.135 17:12:45.020 10/10/2000 268
                                                  [ User [ 37297304
```

(Security negotiation complete for User (37297304
Responder, Inbound SPI = 0x69bc69bd, Outbound SPI = 0x991518b4

SEV=9 IPSECDBG/6 RPT=2 17:12:45.020 10/10/2000 271
,IPSEC key message parse - msgtype 1, Len 536, vers 1, pid 00000000, seq 0
,err 0, type 2, mode 1, state 64, label 0, pad 0, spi 991518b4, encrKeyLen 24
,hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 0
lifetime2 0, dsId 2

SEV=9 IPSECDBG/1 RPT=2 17:12:45.020 10/10/2000 274
!Processing KEY_ADD MSG

SEV=9 IPSECDBG/1 RPT=3 17:12:45.020 10/10/2000 275
key_msghdr2secassoc(): Enter

SEV=7 IPSECDBG/1 RPT=4 17:12:45.020 10/10/2000 276
No USER filter configured

SEV=9 IPSECDBG/1 RPT=5 17:12:45.020 10/10/2000 277
KeyProcessAdd: Enter

SEV=8 IPSECDBG/1 RPT=6 17:12:45.020 10/10/2000 278
KeyProcessAdd: Adding outbound SA

SEV=8 IPSECDBG/1 RPT=7 17:12:45.020 10/10/2000 279
KeyProcessAdd: src 172.18.124.134 mask 0.0.0.0, dst 192.168.1.1 mask 0.0.0.0

SEV=8 IPSECDBG/1 RPT=8 17:12:45.020 10/10/2000 280
KeyProcessAdd: FilterIpsecAddIkeSa success

SEV=9 IPSECDBG/6 RPT=3 17:12:45.020 10/10/2000 281
,IPSEC key message parse - msgtype 3, Len 292, vers 1, pid 00000000, seq 0
,err 0, type 2, mode 1, state 32, label 0, pad 0, spi 69bc69bd, encrKeyLen 24
,hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 0
lifetime2 0, dsId 2

SEV=9 IPSECDBG/1 RPT=9 17:12:45.020 10/10/2000 284
!Processing KEY_UPDATE MSG

SEV=9 IPSECDBG/1 RPT=10 17:12:45.020 10/10/2000 285
Update inbound SA addresses

SEV=9 IPSECDBG/1 RPT=11 17:12:45.020 10/10/2000 286
key_msghdr2secassoc(): Enter

SEV=7 IPSECDBG/1 RPT=12 17:12:45.020 10/10/2000 287
No USER filter configured

SEV=9 IPSECDBG/1 RPT=13 17:12:45.020 10/10/2000 288
KeyProcessUpdate: Enter
SEV=8 IPSECDBG/1 RPT=14 17:12:45.020 10/10/2000 289
KeyProcessUpdate: success

SEV=8 IKEDBG/7 RPT=1 17:12:45.020 10/10/2000 290
IKE got a KEY_ADD MSG for SA: SPI = 0x991518b4

SEV=8 IKEDBG/0 RPT=51 17:12:45.020 10/10/2000 291
pitcher: rcv KEY_UPDATE, spi 0x69bc69bd

تصحيح أخطاء IPSec بشكل جيد باستخدام المصادقة المحلية

SEV=8 IKEDECODE/0 RPT=1 161.44.17.135 17:12:32.560 10/10/2000 1
(ISAKMP HEADER : (Version 1.0

```
                        Initiator Cookie(8):  9D F3 34 FE 89 BF AA B2
                        Responder Cookie(8):  00 00 00 00 00 00 00 00
                                    (Next Payload  :       SA (1
                         Exchange Type :       Oakley Aggressive Mode
                                       Flags         :       0
                                       Message ID    :       0
                                    Length        :       307

          SEV=8 IKEDBG/0 RPT=1 161.44.17.135 17:12:32.560 10/10/2000 7
                              : RECEIVED Message (msgid=0) with payloads
(HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + VENDOR (13) + NONE (0
                                              total length : 307 ...

         SEV=9 IKEDBG/0 RPT=2 161.44.17.135 17:12:32.560 10/10/2000 10
                                               processing SA payload

      SEV=8 IKEDECODE/0 RPT=2 161.44.17.135 17:12:32.560 10/10/2000 11
                                                  : SA Payload Decode
                                    (DOI           :       IPSEC (1
                               (Situation     :       Identity Only (1
                                           Length        :       120

      SEV=8 IKEDECODE/0 RPT=3 161.44.17.135 17:12:32.560 10/10/2000 14
                                                    :Proposal Decode
                                             Proposal #    :       1
                                      (Protocol ID   :       ISAKMP (1
                                               of Transforms:       4#
                                    Spi           :       00 00 00 00
                                           Length        :       108

      SEV=8 IKEDECODE/0 RPT=4 161.44.17.135 17:12:32.560 10/10/2000 18
                                  :Transform # 1 Decode for Proposal # 1
                                               Transform #   :       1
                                        (Transform ID  :       IKE (1
                                             Length        :       24

      SEV=8 IKEDECODE/0 RPT=5 161.44.17.135 17:12:32.560 10/10/2000 20
                           :Phase 1 SA Attribute Decode for Transform # 1
                                    (Encryption Alg:       DES-CBC (1
                                        (Hash Alg      :       MD5 (1
                                (DH Group      :       Oakley Group 1 (1
                                 (Auth Method   :       Preshared Key (1

      SEV=8 IKEDECODE/0 RPT=6 161.44.17.135 17:12:32.560 10/10/2000 24
                                  :Transform # 2 Decode for Proposal # 1
                                               Transform #   :       2
                                        (Transform ID  :       IKE (1
                                             Length        :       24

      SEV=8 IKEDECODE/0 RPT=7 161.44.17.135 17:12:32.560 10/10/2000 26
                           :Phase 1 SA Attribute Decode for Transform # 2
                                    (Encryption Alg:       Triple-DES (5
                                        (Hash Alg      :       MD5 (1
                                (DH Group      :       Oakley Group 1 (1
                                 (Auth Method   :       Preshared Key (1

      SEV=8 IKEDECODE/0 RPT=8 161.44.17.135 17:12:32.560 10/10/2000 30
                                  :Transform # 3 Decode for Proposal # 1
                                               Transform #   :       3
                                        (Transform ID  :       IKE (1
                                             Length        :       24

      SEV=8 IKEDECODE/0 RPT=9 161.44.17.135 17:12:32.560 10/10/2000 32
                           :Phase 1 SA Attribute Decode for Transform # 3
```

```
                                (Encryption Alg:       Triple-DES (5
                                       (Hash Alg      :       SHA (2
                                (DH Group      :       Oakley Group 1 (1
                                 (Auth Method   :       Preshared Key (1

SEV=8 IKEDECODE/0 RPT=10 161.44.17.135 17:12:32.560 10/10/2000 36
                                :Transform # 4 Decode for Proposal # 1
                                             Transform #   :       4
                                       (Transform ID  :       IKE (1
                                            Length        :       24

SEV=8 IKEDECODE/0 RPT=11 161.44.17.135 17:12:32.560 10/10/2000 38
                                 :Phase 1 SA Attribute Decode for Transform # 4
                                          (Encryption Alg:       DES-CBC (1
                                       (Hash Alg      :       SHA (2
                                (DH Group      :       Oakley Group 1 (1
                                 (Auth Method   :       Preshared Key (1

    SEV=8 IKEDBG/0 RPT=3 161.44.17.135 17:12:32.560 10/10/2000 42
                         Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
                                                :Parsing received transform
                      :Phase 1 failure against global IKE proposal # 1
                             :Mismatched attr types for class DH Group
                                               Rcv'd: Oakley Group 1
                                               Cfg'd: Oakley Group 2

    SEV=8 IKEDBG/0 RPT=4 161.44.17.135 17:12:32.560 10/10/2000 47
                      :Phase 1 failure against global IKE proposal # 2
                       :Mismatched attr types for class Encryption Alg
                                                    Rcv'd: DES-CBC
                                                Cfg'd: Triple-DES

    SEV=8 IKEDBG/0 RPT=5 161.44.17.135 17:12:32.560 10/10/2000 50
                         Proposal # 1, Transform # 2, Type ISAKMP, Id IKE
                                                :Parsing received transform
                      :Phase 1 failure against global IKE proposal # 1
                             :Mismatched attr types for class DH Group
                                               Rcv'd: Oakley Group 1
                                               Cfg'd: Oakley Group 2

    SEV=8 IKEDBG/0 RPT=6 161.44.17.135 17:12:32.560 10/10/2000 55
                         Proposal # 1, Transform # 3, Type ISAKMP, Id IKE
                                                :Parsing received transform
                      :Phase 1 failure against global IKE proposal # 1
                             :Mismatched attr types for class DH Group
                                               Rcv'd: Oakley Group 1
                                               Cfg'd: Oakley Group 2

    SEV=8 IKEDBG/0 RPT=7 161.44.17.135 17:12:32.560 10/10/2000 60
                      :Phase 1 failure against global IKE proposal # 2
                             :Mismatched attr types for class Hash Alg
                                                      Rcv'd: SHA
                                                      Cfg'd: MD5

    SEV=8 IKEDBG/0 RPT=8 161.44.17.135 17:12:32.560 10/10/2000 62
                      :Phase 1 failure against global IKE proposal # 3
                       :Mismatched attr types for class Encryption Alg
                                                   Rcv'd: Triple-DES
                                                      Cfg'd: DES-CBC

    SEV=8 IKEDBG/0 RPT=9 161.44.17.135 17:12:32.560 10/10/2000 65
                         Proposal # 1, Transform # 4, Type ISAKMP, Id IKE
                                                :Parsing received transform
                      :Phase 1 failure against global IKE proposal # 1
```

```
                    :Mismatched attr types for class DH Group
                                    Rcv'd: Oakley Group 1
                                    Cfg'd: Oakley Group 2

SEV=8 IKEDBG/0 RPT=10 161.44.17.135 17:12:32.560 10/10/2000 70
            :Phase 1 failure against global IKE proposal # 2
             :Mismatched attr types for class Encryption Alg
                                       Rcv'd: DES-CBC
                                    Cfg'd: Triple-DES

SEV=8 IKEDBG/0 RPT=11 161.44.17.135 17:12:32.560 10/10/2000 73
            :Phase 1 failure against global IKE proposal # 3
                   :Mismatched attr types for class Hash Alg
                                          Rcv'd: SHA
                                          Cfg'd: MD5

SEV=7 IKEDBG/0 RPT=12 161.44.17.135 17:12:32.560 10/10/2000 75
                                  Oakley proposal is acceptable

SEV=9 IKEDBG/0 RPT=13 161.44.17.135 17:12:32.560 10/10/2000 76
                                       processing ke payload

SEV=9 IKEDBG/0 RPT=14 161.44.17.135 17:12:32.560 10/10/2000 77
                                          processing ISA_KE

 SEV=9 IKEDBG/1 RPT=1 161.44.17.135 17:12:32.560 10/10/2000 78
                                     processing nonce payload

 SEV=9 IKEDBG/1 RPT=2 161.44.17.135 17:12:32.560 10/10/2000 79
                                           Processing ID

 SEV=9 IKEDBG/1 RPT=3 161.44.17.135 17:12:32.560 10/10/2000 80
                                     processing vid payload

SEV=9 IKEDBG/23 RPT=1 161.44.17.135 17:12:32.580 10/10/2000 81
                  Starting group lookup for peer 161.44.17.135

SEV=7 IKEDBG/0 RPT=15 161.44.17.135 17:12:32.680 10/10/2000 82
                                  (Found Phase 1 Group (vpn3000

SEV=7 IKEDBG/14 RPT=1 161.44.17.135 17:12:32.680 10/10/2000 83
                        Authentication configured for Internal

SEV=9 IKEDBG/0 RPT=16 161.44.17.135 17:12:32.680 10/10/2000 84
                                 constructing ISA_SA for isakmp

SEV=9 IKEDBG/0 RPT=17 161.44.17.135 17:12:32.680 10/10/2000 85
                                     constructing ke payload

 SEV=9 IKEDBG/1 RPT=4 161.44.17.135 17:12:32.680 10/10/2000 86
                                   constructing nonce payload

    SEV=9 IKE/0 RPT=1 161.44.17.135 17:12:32.680 10/10/2000 87
                                ...Generating keys for Responder

 SEV=9 IKEDBG/1 RPT=5 161.44.17.135 17:12:32.680 10/10/2000 88
                                           constructing ID

              SEV=9 IKEDBG/0 RPT=18 17:12:32.680 10/10/2000 89
                                     construct hash payload

SEV=9 IKEDBG/0 RPT=19 161.44.17.135 17:12:32.680 10/10/2000 90
                                           computing hash
```

```
SEV=9 IKEDBG/1 RPT=6 161.44.17.135 17:12:32.680 10/10/2000 91
                                        constructing vid payload

SEV=8 IKEDBG/0 RPT=20 161.44.17.135 17:12:32.680 10/10/2000 92
                          : SENDING Message (msgid=0) with payloads
                               HDR + SA (1)  ... total length : 248

SEV=8 IKEDECODE/0 RPT=12 161.44.17.135 17:12:32.730 10/10/2000 93
                                ( ISAKMP HEADER :         ( Version 1.0
                        Initiator Cookie(8):  9D F3 34 FE 89 BF AA B2
                        Responder Cookie(8):  B7 AD 34 D2 74 4D 05 DA
                                      (Next Payload  :       HASH (8
                         Exchange Type :       Oakley Aggressive Mode
                                 ( Flags         :       1   (ENCRYPT
                                              Message ID    :       0
                                             Length        :       52

SEV=8 IKEDBG/0 RPT=21 161.44.17.135 17:12:32.730 10/10/2000 99
                               : RECEIVED Message (msgid=0) with payloads
                        HDR + HASH (8) + NONE (0) ... total length : 48

SEV=9 IKEDBG/0 RPT=22 161.44.17.135 17:12:32.730 10/10/2000 101
                                                  processing hash

SEV=9 IKEDBG/0 RPT=23 161.44.17.135 17:12:32.730 10/10/2000 102
                                                  computing hash

SEV=8 IKEDECODE/0 RPT=13 161.44.17.135 17:12:33.410 10/10/2000 103
                                ( ISAKMP HEADER :         ( Version 1.0
                        Initiator Cookie(8):  9D F3 34 FE 89 BF AA B2
                        Responder Cookie(8):  B7 AD 34 D2 74 4D 05 DA
                                      (Next Payload  :       HASH (8
                              Exchange Type :       Oakley Quick Mode
                                 ( Flags         :       1   (ENCRYPT
                                      Message ID    :       48687ca1
                                           Length        :       308

SEV=9 IKEDBG/21 RPT=1 161.44.17.135 17:12:33.410 10/10/2000 110
 Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress

SEV=9 IKEDBG/0 RPT=24 161.44.17.135 17:12:33.410 10/10/2000 111
                                        constructing blank hash

SEV=9 IKEDBG/0 RPT=25 161.44.17.135 17:12:33.410 10/10/2000 112
                                           constructing qm hash

SEV=8 IKEDBG/0 RPT=26 161.44.17.135 17:12:33.410 10/10/2000 113
                        : SENDING Message (msgid=fc2ce5eb) with payloads
                                  HDR + HASH (8)  ... total length : 68

SEV=8 IKEDECODE/0 RPT=14 161.44.17.135 17:12:44.680 10/10/2000 115
                                ( ISAKMP HEADER :         ( Version 1.0
                        Initiator Cookie(8):  9D F3 34 FE 89 BF AA B2
                        Responder Cookie(8):  B7 AD 34 D2 74 4D 05 DA
                                      (Next Payload  :       HASH (8
                           Exchange Type :       Oakley Transactional
                                 ( Flags         :       1   (ENCRYPT
                                      Message ID    :       fc2ce5eb
                                            Length        :       92

SEV=8 IKEDBG/0 RPT=27 161.44.17.135 17:12:44.680 10/10/2000 122
                       : RECEIVED Message (msgid=fc2ce5eb) with payloads
           HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 85
```

```
                                    SEV=9 IKEDBG/1 RPT=7 17:12:44.680 10/10/2000 124
                                                        !process_attr(): Enter

                                    SEV=9 IKEDBG/1 RPT=8 17:12:44.680 10/10/2000 125
                                                    .Processing cfg reply attributes

                          SEV=7 IKEDBG/14 RPT=2 161.44.17.135 17:12:44.980 10/10/2000 126
                                                                [ User [ 37297304
                                                Authentication configured for Internal

                             SEV=4 IKE/52 RPT=7 161.44.17.135 17:12:44.980 10/10/2000 127
                                                                [ User [ 37297304
                                                  .User (37297304) authenticated

                          SEV=9 IKEDBG/31 RPT=1 161.44.17.135 17:12:44.980 10/10/2000 128
                                                                [ User [ 37297304
(Obtained IP addr (192.168.1.1) prior to initiating Mode Cfg (XAuth enabled

                          SEV=9 IKEDBG/0 RPT=28 161.44.17.135 17:12:44.980 10/10/2000 130
                                                                [ User [ 37297304
                                                            constructing blank hash

                          SEV=9 IKEDBG/0 RPT=29 161.44.17.135 17:12:44.980 10/10/2000 131
                            ............                C0A80101 F0010000 00010004 :0000

                          SEV=9 IKEDBG/0 RPT=30 161.44.17.135 17:12:44.980 10/10/2000 132
                                                                [ User [ 37297304
                                                             constructing QM hash

                          SEV=8 IKEDBG/0 RPT=31 161.44.17.135 17:12:44.980 10/10/2000 133
                                        : SENDING Message (msgid=fc2ce5eb) with payloads
                                                    HDR + HASH (8)  ... total length : 80

                    SEV=8 IKEDECODE/0 RPT=15 161.44.17.135 17:12:44.990 10/10/2000 135
                                                     ( ISAKMP HEADER :         ( Version 1.0
                                                Initiator Cookie(8):  9D F3 34 FE 89 BF AA B2
                                                Responder Cookie(8):  B7 AD 34 D2 74 4D 05 DA
                                                           (Next Payload  :       HASH (8
                                              Exchange Type :       Oakley Transactional
                                                    ( Flags         :       1   (ENCRYPT
                                                         Message ID    :       fc2ce5eb
                                                               Length        :       68

                          SEV=8 IKEDBG/0 RPT=32 161.44.17.135 17:12:44.990 10/10/2000 142
                                        : RECEIVED Message (msgid=fc2ce5eb) with payloads
                             HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 64

                                    SEV=9 IKEDBG/1 RPT=9 17:12:44.990 10/10/2000 144
                                                        !process_attr(): Enter

                                   SEV=9 IKEDBG/1 RPT=10 17:12:44.990 10/10/2000 145
                                                    Processing cfg ACK attributes

                                   SEV=9 IKEDBG/1 RPT=11 17:12:44.990 10/10/2000 146
                                                     !Received IPV4 address ack

                                   SEV=9 IKEDBG/1 RPT=12 17:12:44.990 10/10/2000 147
                                                         !Received Save PW ack

                                    SEV=4 AUTH/21 RPT=18 17:12:44.990 10/10/2000 148
                                                        User 37297304 connected

                          SEV=7 IKEDBG/22 RPT=1 161.44.17.135 17:12:44.990 10/10/2000 149
                                                                [ User [ 37297304
```

```
                    Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed

                    SEV=8 IKEDBG/0 RPT=33 161.44.17.135 17:12:44.990 10/10/2000 151
                                    : RECEIVED Message (msgid=48687ca1) with payloads
(HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0
                                                        total length : 304 ...

                    SEV=9 IKEDBG/0 RPT=34 161.44.17.135 17:12:44.990 10/10/2000 154
                                                              [ User [ 37297304
                                                                processing hash

                    SEV=9 IKEDBG/0 RPT=35 161.44.17.135 17:12:44.990 10/10/2000 155
                                                              [ User [ 37297304
                                                            processing SA payload

                SEV=8 IKEDECODE/0 RPT=16 161.44.17.135 17:12:44.990 10/10/2000 156
                                                             : SA Payload Decode
                                              (DOI           :       IPSEC (1
                                         (Situation     :       Identity Only (1
                                                      Length        :       180

                SEV=8 IKEDECODE/0 RPT=17 161.44.17.135 17:12:44.990 10/10/2000 159
                                                                  :Proposal Decode
                                                    Proposal #    :       1
                                               (Protocol ID   :       ESP (3
                                                    of Transforms:       1#
                                           Spi           :       99 15 18 B4
                                                    Length        :       28

                SEV=8 IKEDECODE/0 RPT=18 161.44.17.135 17:12:44.990 10/10/2000 163
                                        :Transform # 1 Decode for Proposal # 1
                                                    Transform #   :       1
                                       (Transform ID  :       DES-CBC (2
                                                    Length        :       16

                SEV=8 IKEDECODE/0 RPT=19 161.44.17.135 17:12:44.990 10/10/2000 165
                                 :Phase 2 SA Attribute Decode for Transform # 1
                                                (HMAC Algorithm:       MD5 (1
                                             (Encapsulation :       Tunnel (1

                SEV=8 IKEDECODE/0 RPT=20 161.44.17.135 17:12:44.990 10/10/2000 167
                                                                  :Proposal Decode
                                                    Proposal #    :       2
                                               (Protocol ID   :       ESP (3
                                                    of Transforms:       1#
                                           Spi           :       99 15 18 B4
                                                    Length        :       28

                SEV=8 IKEDECODE/0 RPT=21 161.44.17.135 17:12:44.990 10/10/2000 171
                                        :Transform # 1 Decode for Proposal # 2
                                                    Transform #   :       1
                                       (Transform ID  :       Triple-DES (3
                                                    Length        :       16

                SEV=8 IKEDECODE/0 RPT=22 161.44.17.135 17:12:44.990 10/10/2000 173
                                 :Phase 2 SA Attribute Decode for Transform # 1
                                                (HMAC Algorithm:       MD5 (1
                                             (Encapsulation :       Tunnel (1

                SEV=8 IKEDECODE/0 RPT=23 161.44.17.135 17:12:44.990 10/10/2000 175
                                                                  :Proposal Decode
                                                    Proposal #    :       3
                                               (Protocol ID   :       ESP (3
                                                    of Transforms:       1#
```

```
                                    Spi           :       99 15 18 B4
                                            Length        :       28

SEV=8 IKEDECODE/0 RPT=24 161.44.17.135 17:12:44.990 10/10/2000 179
                                :Transform # 1 Decode for Proposal # 3
                                            Transform #   :       1
                                   (Transform ID  :       DES-CBC (2
                                            Length        :       16

SEV=8 IKEDECODE/0 RPT=25 161.44.17.135 17:12:44.990 10/10/2000 181
                           :Phase 2 SA Attribute Decode for Transform # 1
                                        (HMAC Algorithm:       SHA (2
                                     (Encapsulation :       Tunnel (1

SEV=8 IKEDECODE/0 RPT=26 161.44.17.135 17:12:44.990 10/10/2000 183
                                                        :Proposal Decode
                                             Proposal #    :       4
                                        (Protocol ID   :       ESP (3
                                             of Transforms:       1#
                                    Spi           :       99 15 18 B4
                                            Length        :       28

SEV=8 IKEDECODE/0 RPT=27 161.44.17.135 17:12:44.990 10/10/2000 187
                                :Transform # 1 Decode for Proposal # 4
                                            Transform #   :       1
                                  (Transform ID  :       Triple-DES (3
                                            Length        :       16

SEV=8 IKEDECODE/0 RPT=28 161.44.17.135 17:12:44.990 10/10/2000 189
                           :Phase 2 SA Attribute Decode for Transform # 1
                                        (HMAC Algorithm:       SHA (2
                                     (Encapsulation :       Tunnel (1

SEV=8 IKEDECODE/0 RPT=29 161.44.17.135 17:12:44.990 10/10/2000 191
                                                        :Proposal Decode
                                             Proposal #    :       5
                                        (Protocol ID   :       ESP (3
                                             of Transforms:       1#
                                    Spi           :       99 15 18 B4
                                            Length        :       28

SEV=8 IKEDECODE/0 RPT=30 161.44.17.135 17:12:44.990 10/10/2000 195
                                :Transform # 1 Decode for Proposal # 5
                                            Transform #   :       1
                                     (Transform ID  :       NULL (11
                                            Length        :       16

SEV=8 IKEDECODE/0 RPT=31 161.44.17.135 17:12:44.990 10/10/2000 197
                           :Phase 2 SA Attribute Decode for Transform # 1
                                        (HMAC Algorithm:       MD5 (1
                                     (Encapsulation :       Tunnel (1

SEV=8 IKEDECODE/0 RPT=32 161.44.17.135 17:12:44.990 10/10/2000 199
                                                        :Proposal Decode
                                             Proposal #    :       6
                                        (Protocol ID   :       ESP (3
                                             of Transforms:       1#
                                    Spi           :       99 15 18 B4
                                            Length        :       28

SEV=8 IKEDECODE/0 RPT=33 161.44.17.135 17:12:44.990 10/10/2000 203
                                :Transform # 1 Decode for Proposal # 6
                                            Transform #   :       1
                                     (Transform ID  :       NULL (11
```

```
                                                Length        :       16

     SEV=8 IKEDECODE/0 RPT=34 161.44.17.135 17:12:44.990 10/10/2000 205
                          :Phase 2 SA Attribute Decode for Transform # 1
                                        (HMAC Algorithm:       SHA (2
                                     (Encapsulation :       Tunnel (1

        SEV=9 IKEDBG/1 RPT=13 161.44.17.135 17:12:44.990 10/10/2000 207
                                                        [ User [ 37297304
                                                  processing nonce payload

        SEV=9 IKEDBG/1 RPT=14 161.44.17.135 17:12:44.990 10/10/2000 208
                                                        [ User [ 37297304
                                                      Processing ID

          SEV=5 IKE/25 RPT=13 161.44.17.135 17:12:44.990 10/10/2000 209
                                                        [ User [ 37297304
                                  :Received remote Proxy Host data in ID Payload
                                       Address 161.44.17.135, Protocol 0, Port 0

        SEV=7 IKEDBG/1 RPT=15 161.44.17.135 17:12:44.990 10/10/2000 212
                                                        [ User [ 37297304
                                          !Modifying client proxy src address

        SEV=9 IKEDBG/1 RPT=16 161.44.17.135 17:12:44.990 10/10/2000 213
                                                        [ User [ 37297304
                                                      Processing ID

           SEV=5 IKE/24 RPT=7 161.44.17.135 17:12:44.990 10/10/2000 214
                                                        [ User [ 37297304
                                    :Received local Proxy Host data in ID Payload
                                       Address 172.18.124.134, Protocol 0, Port 0

        SEV=9 IKEDBG/0 RPT=36 161.44.17.135 17:12:44.990 10/10/2000 217
                                                        [ User [ 37297304
                                                Processing Notify payload

     SEV=8 IKEDECODE/0 RPT=35 161.44.17.135 17:12:44.990 10/10/2000 218
                                                  : Notify Payload Decode
                                          (DOI           :       IPSEC (1
                                        (Protocol      :       ISAKMP (1
                              (Message       :       Initial contact (24578
Spi           :       9D F3 34 FE 89 BF AA B2 B7 AD 34 D2 74 4D 05 DA
                                                Length        :       28

                             SEV=8 IKEDBG/0 RPT=37 17:12:44.990 10/10/2000 224
                                        QM IsRekeyed old sa not found by addr

          SEV=5 IKE/66 RPT=13 161.44.17.135 17:12:44.990 10/10/2000 225
                                                        [ User [ 37297304
                                IKE Remote Peer configured for SA: ESP-3DES-MD5

        SEV=9 IKEDBG/0 RPT=38 161.44.17.135 17:12:44.990 10/10/2000 226
                                                        [ User [ 37297304
                                                     processing IPSEC SA

                             SEV=8 IKEDBG/0 RPT=39 17:12:44.990 10/10/2000 227
                             Proposal # 1, Transform # 1, Type ESP, Id DES-CBC
                                                  :Parsing received transform
                                                      :Phase 2 failure
                                  :Mismatched transform IDs for protocol ESP
                                                        Rcv'd: DES-CBC
                                                    Cfg'd: Triple-DES
```

```
SEV=7 IKEDBG/27 RPT=1 161.44.17.135 17:12:45.000 10/10/2000 232
                                                    [ User [ 37297304
                        IPSec SA Proposal # 2, Transform # 1 acceptable

SEV=7 IKEDBG/0 RPT=40 161.44.17.135 17:12:45.000 10/10/2000 233
                                                    [ User [ 37297304
                                                !IKE: requesting SPI

                                  SEV=6 IKE/0 RPT=2 17:12:45.000 10/10/2000 234
          AM received unexpected event EV_ACTIVATE_NEW_SA in state AM_ACTIVE

                                  SEV=9 IPSECDBG/6 RPT=1 17:12:45.000 10/10/2000 235
 ,IPSEC key message parse - msgtype 6, len 164, vers 1, pid 00000000, seq 13
,err 0, type 2, mode 0, state 32, label 0, pad 0, spi 00000000, encrKeyLen 0
         ,hashKeyLen 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 300
                                                lifetime2 2000000000, dsId 2

                                  SEV=9 IPSECDBG/1 RPT=1 17:12:45.000 10/10/2000 239
                                                !Processing KEY_GETSPI msg

                                 SEV=7 IPSECDBG/13 RPT=1 17:12:45.000 10/10/2000 240
                                                   Reserved SPI 1773955517

                                    SEV=8 IKEDBG/6 RPT=1 17:12:45.000 10/10/2000 241
                                      IKE got SPI from key engine: SPI = 0x69bc69bd

SEV=9 IKEDBG/0 RPT=41 161.44.17.135 17:12:45.000 10/10/2000 242
                                                    [ User [ 37297304
                                          oakley constructing quick mode

SEV=9 IKEDBG/0 RPT=42 161.44.17.135 17:12:45.000 10/10/2000 243
                                                    [ User [ 37297304
                                                constructing blank hash

SEV=9 IKEDBG/0 RPT=43 161.44.17.135 17:12:45.000 10/10/2000 244
                                                    [ User [ 37297304
                                           constructing ISA_SA for ipsec

SEV=9 IKEDBG/1 RPT=17 161.44.17.135 17:12:45.000 10/10/2000 245
                                                    [ User [ 37297304
                                       constructing ipsec nonce payload

SEV=9 IKEDBG/1 RPT=18 161.44.17.135 17:12:45.000 10/10/2000 246
                                                    [ User [ 37297304
                                                 constructing proxy ID

SEV=7 IKEDBG/0 RPT=44 161.44.17.135 17:12:45.000 10/10/2000 247
                                                    [ User [ 37297304
                                               :Transmitting Proxy Id
                                    Remote host: 192.168.1.1  Protocol 0  Port 0
                                  Local host:  172.18.124.134  Protocol 0  Port 0

SEV=9 IKEDBG/0 RPT=45 161.44.17.135 17:12:45.000 10/10/2000 251
                                                    [ User [ 37297304
                                                 constructing QM hash

SEV=8 IKEDBG/0 RPT=46 161.44.17.135 17:12:45.000 10/10/2000 252
                                : SENDING Message (msgid=48687ca1) with payloads
                                          HDR + HASH (8)  ... total length : 136

SEV=8 IKEDECODE/0 RPT=36 161.44.17.135 17:12:45.010 10/10/2000 254
                                        ( ISAKMP HEADER :         ( Version 1.0
                                 Initiator Cookie(8):  9D F3 34 FE 89 BF AA B2
                                 Responder Cookie(8):  B7 AD 34 D2 74 4D 05 DA
```

```
                                                (Next Payload  :       HASH (8
                                          Exchange Type :       Oakley Quick Mode
                                             ( Flags         :       1   (ENCRYPT
                                                   Message ID    :       48687ca1
                                                         Length        :       52

                        SEV=8 IKEDBG/0 RPT=47 161.44.17.135 17:12:45.010 10/10/2000 261
                                      : RECEIVED Message (msgid=48687ca1) with payloads
                                        HDR + HASH (8) + NONE (0) ... total length : 48

                        SEV=9 IKEDBG/0 RPT=48 161.44.17.135 17:12:45.010 10/10/2000 263
                                                                [ User [ 37297304
                                                                  processing hash

                        SEV=9 IKEDBG/0 RPT=49 161.44.17.135 17:12:45.010 10/10/2000 264
                                                                [ User [ 37297304
                                                              loading all IPSEC SAs

                        SEV=9 IKEDBG/1 RPT=19 161.44.17.135 17:12:45.010 10/10/2000 265
                                                                [ User [ 37297304
                                                            !Generating Quick Mode Key

                        SEV=9 IKEDBG/1 RPT=20 161.44.17.135 17:12:45.010 10/10/2000 266
                                                                [ User [ 37297304
                                                            !Generating Quick Mode Key

                        SEV=7 IKEDBG/0 RPT=50 161.44.17.135 17:12:45.020 10/10/2000 267
                                                                [ User [ 37297304
                                                                    :Loading host
                                                           Dst: 172.18.124.134
                                                              Src: 192.168.1.1

                          SEV=4 IKE/49 RPT=13 161.44.17.135 17:12:45.020 10/10/2000 268
                                                                [ User [ 37297304
                                        (Security negotiation complete for User (37297304
                         Responder, Inbound SPI = 0x69bc69bd, Outbound SPI = 0x991518b4

                                                SEV=9 IPSECDBG/6 RPT=2 17:12:45.020 10/10/2000 271
           ,IPSEC key message parse - msgtype 1, Len 536, vers 1, pid 00000000, seq 0
        ,err 0, type 2, mode 1, state 64, label 0, pad 0, spi 991518b4, encrKeyLen 24
                    ,hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 0
                                                                lifetime2 0, dsId 2

                                                SEV=9 IPSECDBG/1 RPT=2 17:12:45.020 10/10/2000 274
                                                                    !Processing KEY_ADD MSG

                                                SEV=9 IPSECDBG/1 RPT=3 17:12:45.020 10/10/2000 275
                                                              key_msghdr2secassoc(): Enter

                                                SEV=7 IPSECDBG/1 RPT=4 17:12:45.020 10/10/2000 276
                                                                No USER filter configured

                                                SEV=9 IPSECDBG/1 RPT=5 17:12:45.020 10/10/2000 277
                                                                  KeyProcessAdd: Enter

                                                SEV=8 IPSECDBG/1 RPT=6 17:12:45.020 10/10/2000 278
                                                              KeyProcessAdd: Adding outbound SA

                                                SEV=8 IPSECDBG/1 RPT=7 17:12:45.020 10/10/2000 279
         KeyProcessAdd: src 172.18.124.134 mask 0.0.0.0, dst 192.168.1.1 mask 0.0.0.0

                                                SEV=8 IPSECDBG/1 RPT=8 17:12:45.020 10/10/2000 280
                                                        KeyProcessAdd: FilterIpsecAddIkeSa success
```

```
                                SEV=9 IPSECDBG/6 RPT=3 17:12:45.020 10/10/2000 281
   ,IPSEC key message parse - msgtype 3, Len 292, vers 1, pid 00000000, seq 0
,err 0, type 2, mode 1, state 32, label 0, pad 0, spi 69bc69bd, encrKeyLen 24
           ,hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 0
                                                        lifetime2 0, dsId 2

                                SEV=9 IPSECDBG/1 RPT=9 17:12:45.020 10/10/2000 284
                                                !Processing KEY_UPDATE MSG

                               SEV=9 IPSECDBG/1 RPT=10 17:12:45.020 10/10/2000 285
                                              Update inbound SA addresses

                               SEV=9 IPSECDBG/1 RPT=11 17:12:45.020 10/10/2000 286
                                            key_msghdr2secassoc(): Enter

                               SEV=7 IPSECDBG/1 RPT=12 17:12:45.020 10/10/2000 287
                                              No USER filter configured

                               SEV=9 IPSECDBG/1 RPT=13 17:12:45.020 10/10/2000 288
                                                KeyProcessUpdate: Enter
                               SEV=8 IPSECDBG/1 RPT=14 17:12:45.020 10/10/2000 289
                                              KeyProcessUpdate: success

                                 SEV=8 IKEDBG/7 RPT=1 17:12:45.020 10/10/2000 290
                                  IKE got a KEY_ADD MSG for SA: SPI = 0x991518b4

                                SEV=8 IKEDBG/0 RPT=51 17:12:45.020 10/10/2000 291
                                          pitcher: rcv KEY_UPDATE, spi 0x69bc69bd
```

تصحيح أخطاء جيد مع SDI

تصحيح أخطاء SDI

إذا نجحت (المصادقة الأولى على SDI)

```
U   37297304/vpn3000             000037297304/37297304/11:57:04   10/06/2000
                                                                        372
      L   Node Secret Sent to Client   zekie.cisco.com/11:57:04   10/06/2000
U   37297304/vpn3000             000037297304/37297304/15:57:05   10/06/2000
                                                                        372
      U   PASSCODE Accepted            zekie.cisco.com/11:57:05   10/06/2000
```

إذا نجح (بعد المصادقة الأولى على SDI)

```
16:06:09U    37297304/vpn3000             000037297304/37297304   10/06/2000
                                                                        372
      12:06:09L    PASSCODE Accepted            zekie.cisco.com   10/06/2000
```

تصحيح أخطاء مركز VPN 3000 (قيد الاختبار)

تصحيح أخطاء "اسم الفئة" للمصادقة:

- AUTH
- Authdbg
- أوثديكود

```
                                SEV=8 AUTHDBG/1 RPT=1 14:09:25.000 10/06/2000 4
                                                AUTH_Open() returns 14
```

```
                                        SEV=7 AUTH/12 RPT=1 14:09:25.000 10/06/2000 5
                                           Authentication session opened: handle = 14

                                        SEV=8 AUTHDBG/3 RPT=1 14:09:25.000 10/06/2000 6
                                                        (AUTH_PutAttrTable(14, 5a2aa0

                                        SEV=8 AUTHDBG/5 RPT=1 14:09:25.000 10/06/2000 7
                                                 (AUTH_Authenticate(14, e5187e0, 306bdc

                                       SEV=8 AUTHDBG/59 RPT=1 14:09:25.000 10/06/2000 8
                                                        (AUTH_BindServer(71e097c, 0, 0

                                       SEV=9 AUTHDBG/69 RPT=1 14:09:25.000 10/06/2000 9
                             Auth Server 649ab4 has been bound to ACB 71e097c, sessions = 1

                                       SEV=8 AUTHDBG/65 RPT=1 14:09:25.000 10/06/2000 10
                                                        (AUTH_CreateTimer(71e097c, 0, 0

                                       SEV=9 AUTHDBG/72 RPT=1 14:09:25.000 10/06/2000 11
                                                     Reply timer created: handle = 490011

                                       SEV=8 AUTHDBG/61 RPT=1 14:09:25.000 10/06/2000 12
                                                         (AUTH_BuildMsg(71e097c, 0, 0

                                       SEV=8 AUTHDBG/51 RPT=1 14:09:25.000 10/06/2000 13
                                                                (Sdi_Build(71e097c

                                       SEV=8 AUTHDBG/64 RPT=1 14:09:25.010 10/06/2000 14
                                                        (AUTH_StartTimer(71e097c, 0, 0

                                       SEV=9 AUTHDBG/73 RPT=1 14:09:25.010 10/06/2000 15
                  Reply timer started: handle = 490011, timestamp = 8553930, timeout = 4000

                                       SEV=8 AUTHDBG/62 RPT=1 14:09:25.010 10/06/2000 16
                                                        (AUTH_SndRequest(71e097c, 0, 0

                                       SEV=8 AUTHDBG/52 RPT=1 14:09:25.010 10/06/2000 17

                                                                  (Sdi_Xmt(71e097c

                                       SEV=9 AUTHDBG/71 RPT=1 14:09:25.010 10/06/2000 18
                                                                      xmit_cnt = 1

                                       SEV=8 AUTHDBG/63 RPT=1 14:09:26.080 10/06/2000 19
                                                         (AUTH_RcvReply(71e097c, 0, 0

                                       SEV=8 AUTHDBG/53 RPT=1 14:09:26.080 10/06/2000 20
                                                                  (Sdi_Rcv(71e097c

                                       SEV=8 AUTHDBG/66 RPT=1 14:09:26.080 10/06/2000 21
                                                        (AUTH_DeleteTimer(71e097c, 0, 0

                                       SEV=9 AUTHDBG/74 RPT=1 14:09:26.080 10/06/2000 22
                                Reply timer stopped: handle = 490011, timestamp = 8554037

                                       SEV=8 AUTHDBG/58 RPT=1 14:09:26.080 10/06/2000 23
                                                         (AUTH_Callback(71e097c, 0, 0

                                          SEV=6 AUTH/4 RPT=1 14:09:26.080 10/06/2000 24
                  Authentication successful: handle = 14, server = 172.18.124.99, user = 37297304

                                       SEV=8 AUTHDBG/2 RPT=1 14:09:26.080 10/06/2000 25
                                                                    (AUTH_Close(14
```

```
SEV=8 AUTHDBG/60 RPT=1 14:09:26.080 10/06/2000 26
(AUTH_UnbindServer(71e097c, 0, 0

SEV=9 AUTHDBG/70 RPT=1 14:09:26.080 10/06/2000 27
Auth Server 649ab4 has been unbound from ACB 71e097c, sessions = 0

SEV=8 AUTHDBG/10 RPT=1 14:09:26.080 10/06/2000 28
(AUTH_Int_FreeAuthCB(71e097c

SEV=9 AUTHDBG/19 RPT=1 14:09:26.080 10/06/2000 29
instance = 15, clone_instance = 0

SEV=7 AUTH/13 RPT=1 14:09:26.080 10/06/2000 30
Authentication session closed: handle = 14
```

تصحيح أخطاء غير صحيح

لم يتم تنشيط اسم المستخدم أو المستخدم غير الصحيح على العميل

تصحيح أخطاء SDI

```
16:30:21U junk/vpn3000 10/06/2000
12:30:21L User Not on Client zekie.cisco.com 10/06/2000
```

تصحيح أخطاء VPN 3000

```
SEV=3 AUTH/5 RPT=5 14:20:06.310 10/06/2000 21
Authentication rejected: Reason = Unspecified
handle = 15, server = 172.18.124.99, user = junk
```

اسم مستخدم جيد، رمز مرور غير صحيح

تصحيح أخطاء SDI

```
16:33:07U 37297304/vpn3000   000037297304/37297304 372 10/06/2000
12:33:07L ACCESS DENIED, PASSCODE Incorrect zekie.cisco.com 10/06/2000
```

تصحيح أخطاء VPN 3000

```
SEV=3 AUTH/5 RPT=6 14:22:52.160 10/06/2000 249
Authentication rejected: Reason = Unspecified
handle = 16, server = 172.18.124.99, user = 37297304
```

خادم SDI الذي يتعذر الوصول إليه أو برنامج تشغيل خلفي

تصحيح أخطاء SDI

لا يظهر أي شيء (لم يستلم طلبا)

تصحيح أخطاء VPN 3000

```
SEV=4 AUTH/9 RPT=7 14:28:55.600 10/06/2000 77
Authentication failed: Reason = Network error
handle = 17, server = 172.18.124.99, user = 37297304
```

لم يتم تكوين VPN 3000 كعميل على مربع SDI

تصحيح أخطاء SDI

```
/<-- 17:37:42U --/172.18.124.134 10/06/2000
13:36:42L Client Not Found   zekie.cisco.com 10/06/2000
```

تصحيح أخطاء VPN 3000

```
SEV=3 AUTH/5 RPT=8 15:26:27.440 10/06/2000 113
Authentication rejected: Reason = Unspecified
handle = 21, server = 172.18.124.99, user = 37297304
```

تمت إزالة مركز VPN 3000 كعميل من خادم SDI، ثم أعادت إضافته

حاول خادم SDI إرسال ملف SecurityID لاستبدال الملف القديم، ولكن VPN 3000 كان لديه هذا الملف بالفعل.

رسالة على SDI

```
13:42:18L Node Verification Failed zekie.cisco.com 10/06/2000
```

تصحيح أخطاء VPN 3000

```
SEV=3 AUTH/5 RPT=9 15:32:03.030 10/06/2000 21
Authentication rejected: Reason = Unspecified
handle = 22, server = 172.18.124.99, user = 37297304
```

لحل هذه المشكلة، احذف ملف SecurityID على مركز VPN 3000 بالانتقال إلى **الإدارة > إدارة الملفات > الملفات > SecurityID > حذف**. عند إعادة الاختبار، يقبل مركز الشبكة الخاصة الظاهرية (VPN) 3000 الملف الجديد من خادم SDI. إذا تم تحديد خانة الاختيار **Edit Client > Send Node Secret** على SDI، فلن يتمكن خادم SDI من إكمال التبادل. بمجرد أن يحتوي مركز VPN 3000 على ملف SecurityID، يتم تحديد خانة الاختيار **Send Node Secret**/عدم تحديد متدرج.

معلومات ذات صلة

- تكوين عميل Cisco VPN إلى مركز VPN 3000 باستخدام مصادقة IPSec SDI الإصدار 5.0 والإصدارات الأحدث
- 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).