تكوين نفق IPSec بين عميل Cisco VPN ل VPN 3000 ومكثف Linux

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين نفق IPSec من جهاز كمبيوتر قائم على بيئة Linux يشغل عميل Cisco VPN إلى مركز Cisco VPN 3000 Series Concentrator حتى يمكنك الوصول إلى الشبكة داخل مركز التركيز بشكل آمن.

قبل البدء

الاصطلاحات

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

المتطلبات الأساسية

يستخدم هذا المستند التكوينات التالية:

- تكوين مركز VPN 3000
- تكوين عميل Linux

المكونات المستخدمة

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

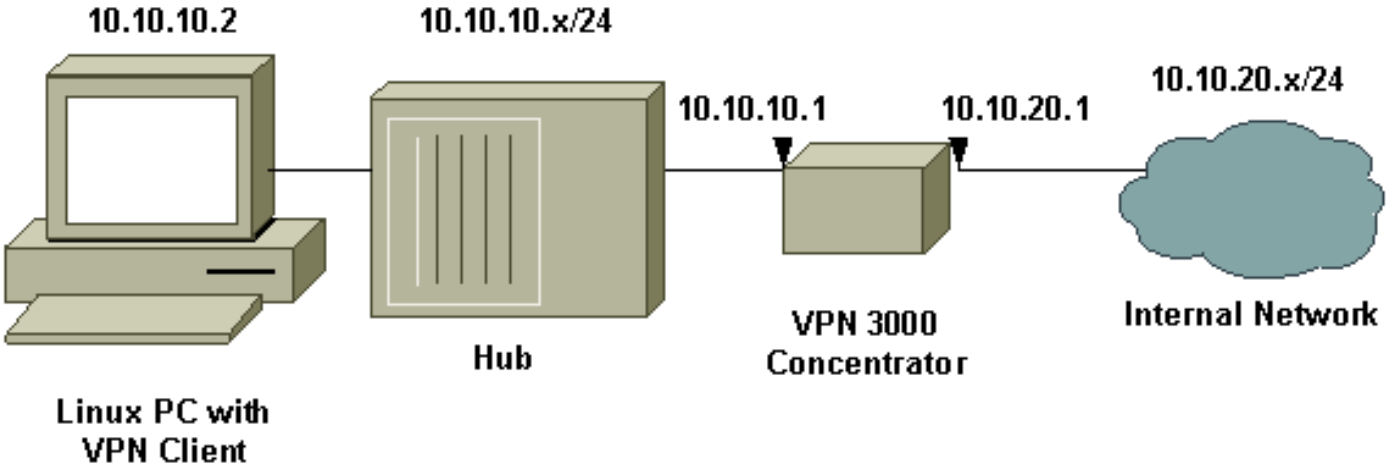
- مركز Cisco VPN 3000، الإصدار x.3
- Cisco VPN Client، الإصدار 3.0.8
- نظام التشغيل Red Hat Linux® الإصدار 7.2 المزود بنواة 10-2.4.7

ملاحظة: يتوفر دعم RedHat8 في إصدارات عميل VPN 3.6.2a والإصدارات الأحدث. يمكن للعملاء المسجلين الحصول على معلومات محددة من خلال البحث في معرف الأخطاء CSCdy49082 (للعملاء المسجلين فقط).

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.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة الموضح في الرسم التخطيطي أدناه.



التكوينات

المهمة

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

تكوين مركز VPN 3000

أستخدم الخطوات التالية لتكوين مركز VPN 3000.

1. قم بالاتصال بمنفذ وحدة تحكم مركز الشبكة الخاصة الظاهرية (VPN) وتحقق من وجود عناوين IP معينة إلى الواجهات الخاصة (الداخلية) والعامة (الخارجية). تحقق أيضا من وجود بوابة افتراضية تم تعيينها بحيث يمكن أن يقوم مركز التركيز بإعادة توجيه الحزم للوجهات التي لا يعلم عنها إلى البوابة الافتراضية.**ملاحظة:** يكون الافتراضي هو عادة موجه عبارة الإنترنت.

```
Configuration (1
Administration (2
Monitoring (3
Save changes to Config file (4
Help Information (5
```

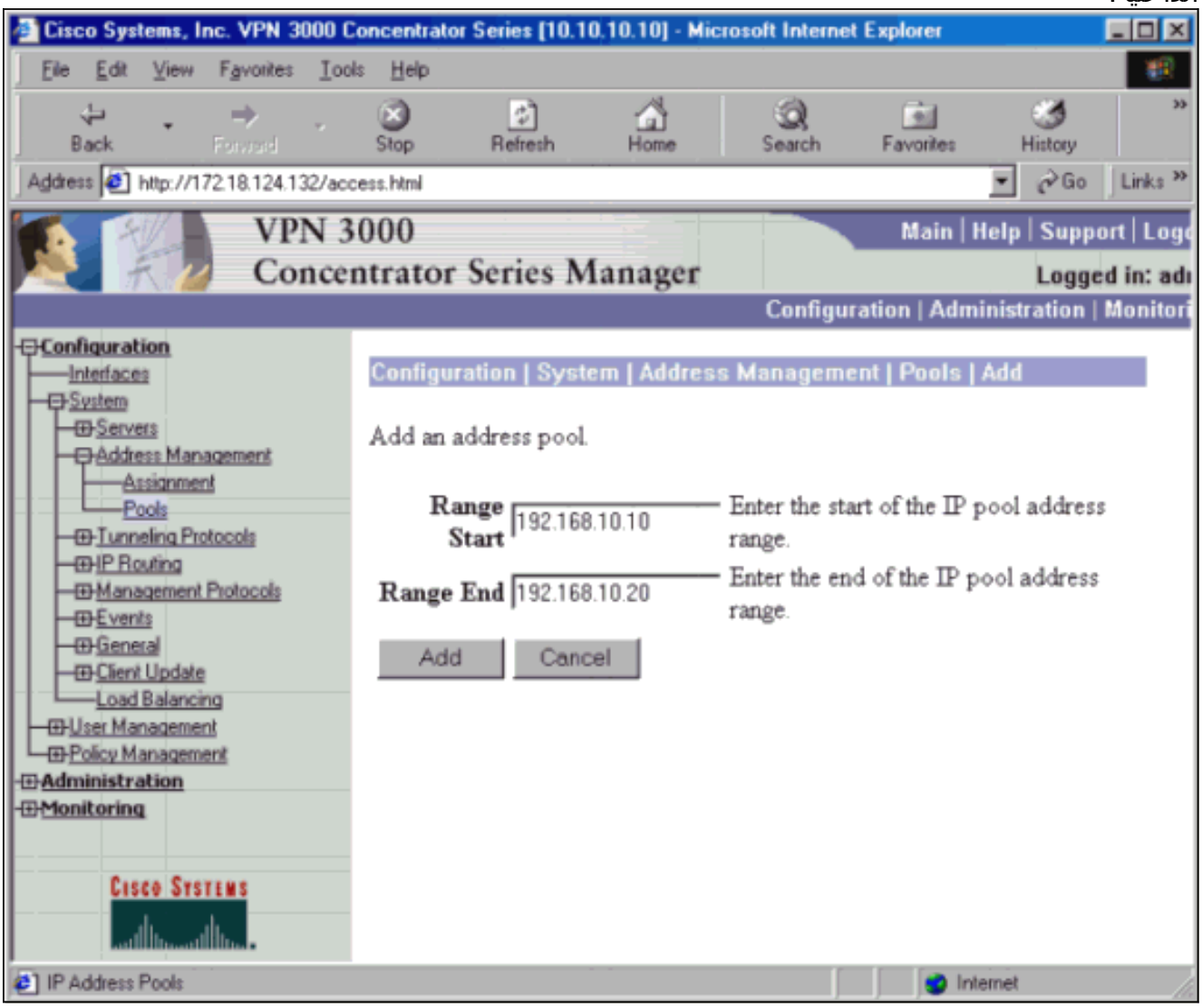
```
                                                                Exit (6

                                                              Main -> 1

                                                  Interface Configuration (1
                                                        System Management (2
                                                          User Management (3
                                                        Policy Management (4
                                                                    Back (5

                                                              Config -> 1
```

يوضح هذا الجدول عناوين IP الحالية.

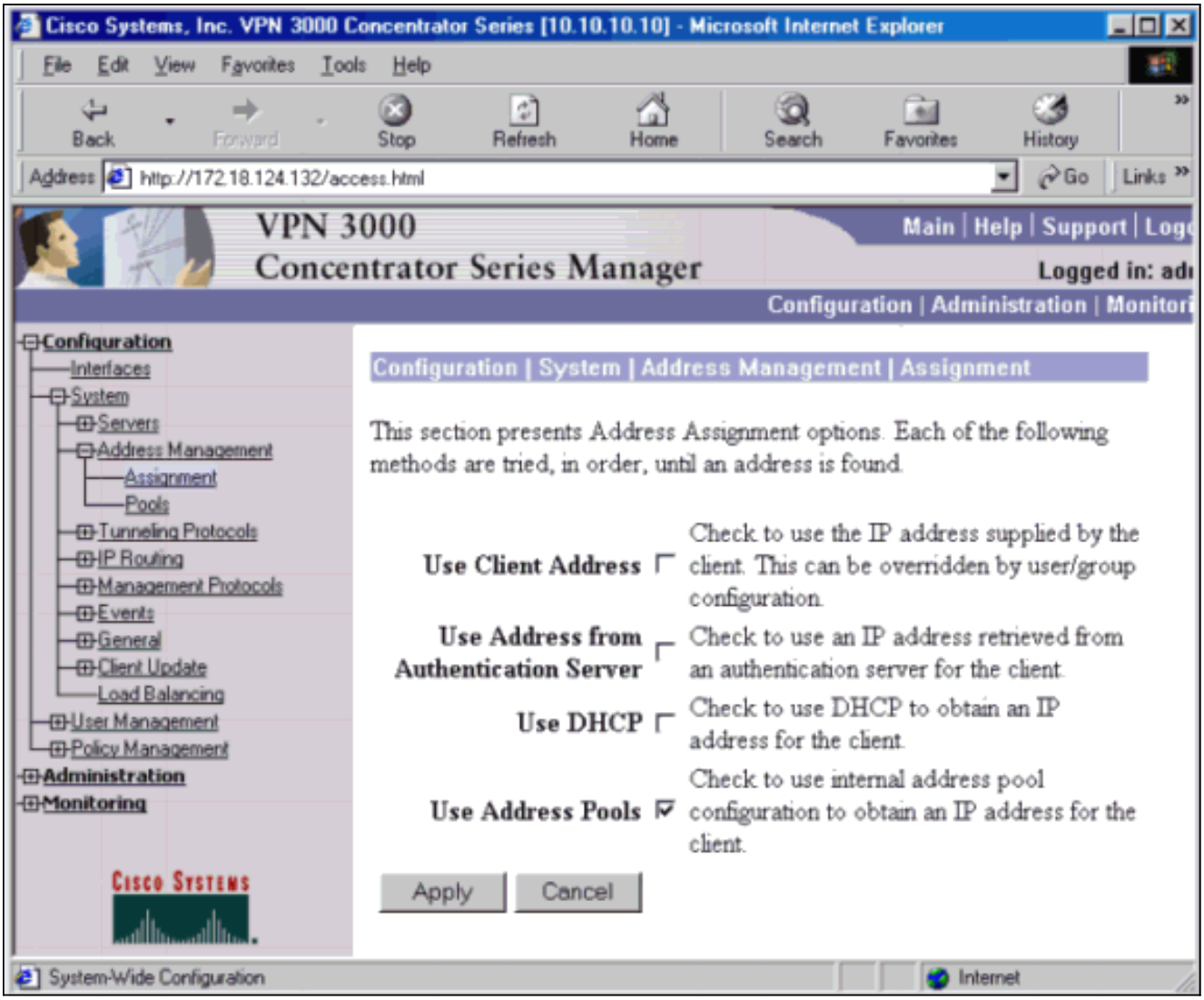
```
     Interface            IP Address/Subnet Mask      MAC Address
-----------------------------------------------------------------------
 Ethernet 1 - Private  | 10.10.20.1/255.255.255.0 | 00.90.A4.00.16.54 |
 Ethernet 2 - Public   | 10.10.10.1/255.255.255.0 | 00.90.A4.00.16.55 |
                   |         Ethernet 3 - External |  0.0.0.0/0.0.0.0 |
-----------------------------------------------------------------------

                                        (Configure Ethernet #1 (Private (1
                                         (Configure Ethernet #2 (Public (2
                                       (Configure Ethernet #3 (External (3
                                               Configure Power Supplies (4
                                              Configure Expansion Cards (5
                                                                    Back (6

                                                          Interfaces -> 6

                                                  Interface Configuration (1
                                                        System Management (2
                                                          User Management (3
                                                        Policy Management (4
                                                                    Back (5

                                                              Config -> 2

                                          (.Servers (Authentication, Accounting, etc (1
                                                             Address Management (2
                                              (.Tunneling Protocols (PPTP, L2TP, etc (3
                                              (.IP Routing (static routes, OSPF, etc (4
                                  (.Management Protocols (Telnet, TFTP, FTP, etc (5
                                                        Event Configuration (6
                                        (.General Config (system name, time, etc (7
                                                                    Back (8

                                                              System -> 4

                                                         Static Routes (1
                                                       Default Gateways (2
                                                                   OSPF (3
                                                             OSPF Areas (4
                                                                   DHCP (5
                                                             Redundancy (6
                                                                   Back (7

                                                             Routing -> 1

                                                          Static Routes
                                                          -------------
                                  Destination     Mask            Metric Destination
                              ------------------------------------------------------
                                        10.10.10.1 1             0.0.0.0         0.0.0.0
```

```
Add Static Route (1
Modify Static Route (2
Delete Static Route (3
Back (4
```

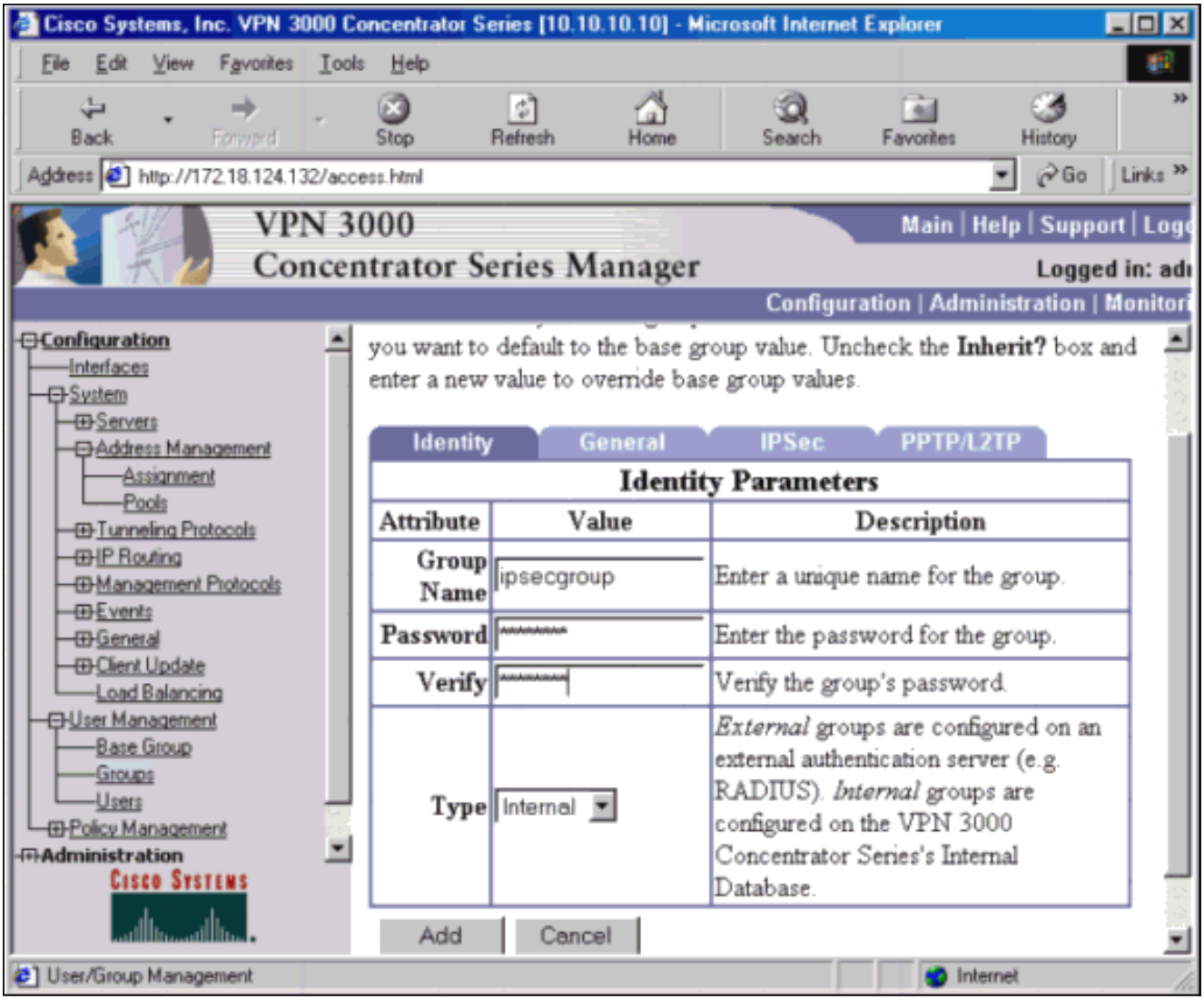
2. لتخصيص نطاق متاح من عناوين IP، قم بتوجيه متصفح إلى الواجهة الداخلية لتمركز VPN 3000 وانتقل إلى **التكوين > النظام > إدارة العناوين > تجمعات > إضافة**. حدد نطاق عناوين IP التي لا تتعارض مع أي أجهزة أخرى على الشبكة
الداخلية.



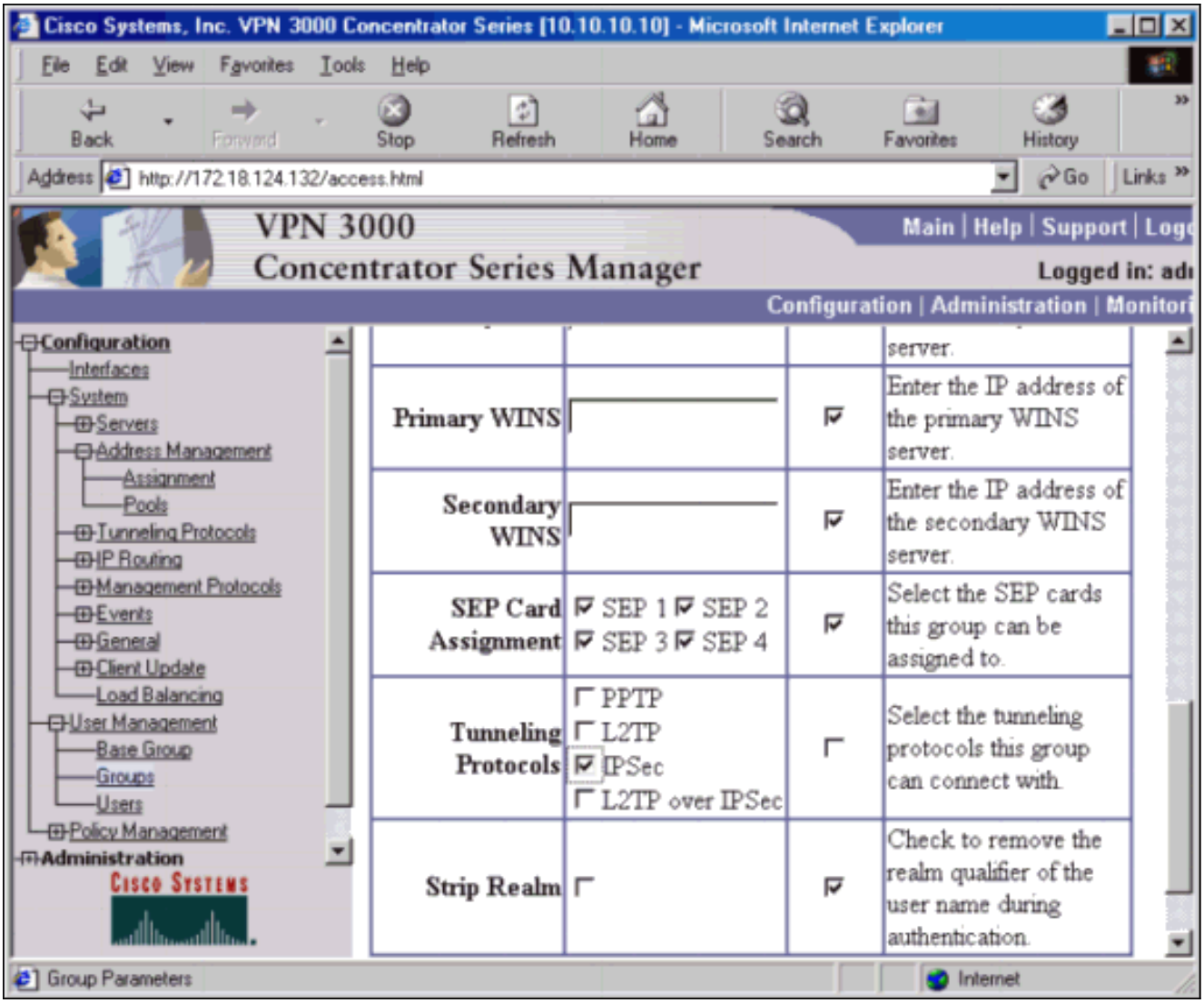
3. ولإعلام مركز الشبكة الخاصة الظاهرية (VPN) باستخدام المجموعة، انتقل إلى **التكوين > النظام > إدارة العناوين > التعيين**، وحدد المربع **إستخدام تجمعات العناوين**.



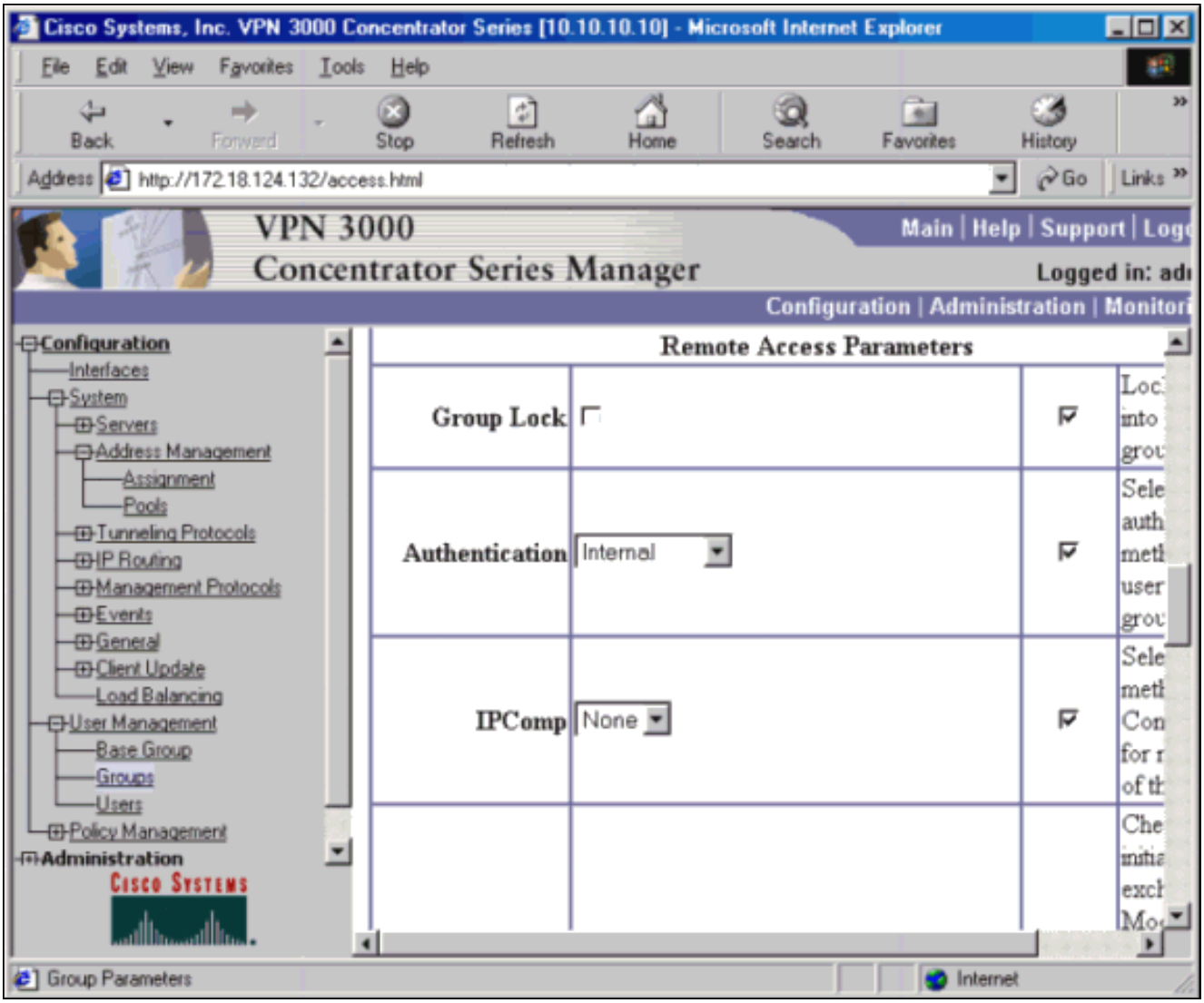
4. قم بتكوين مجموعة IPSec للمستخدمين بالانتقال إلى **التكوين > إدارة المستخدم > مجموعات > إضافة** وتعريف اسم مجموعة وكلمة مرور. يستخدم المثال التالي اسم المجموعة "ipsecgroup" مع كلمة المرور/التحقق على هيئة "Cisco123".



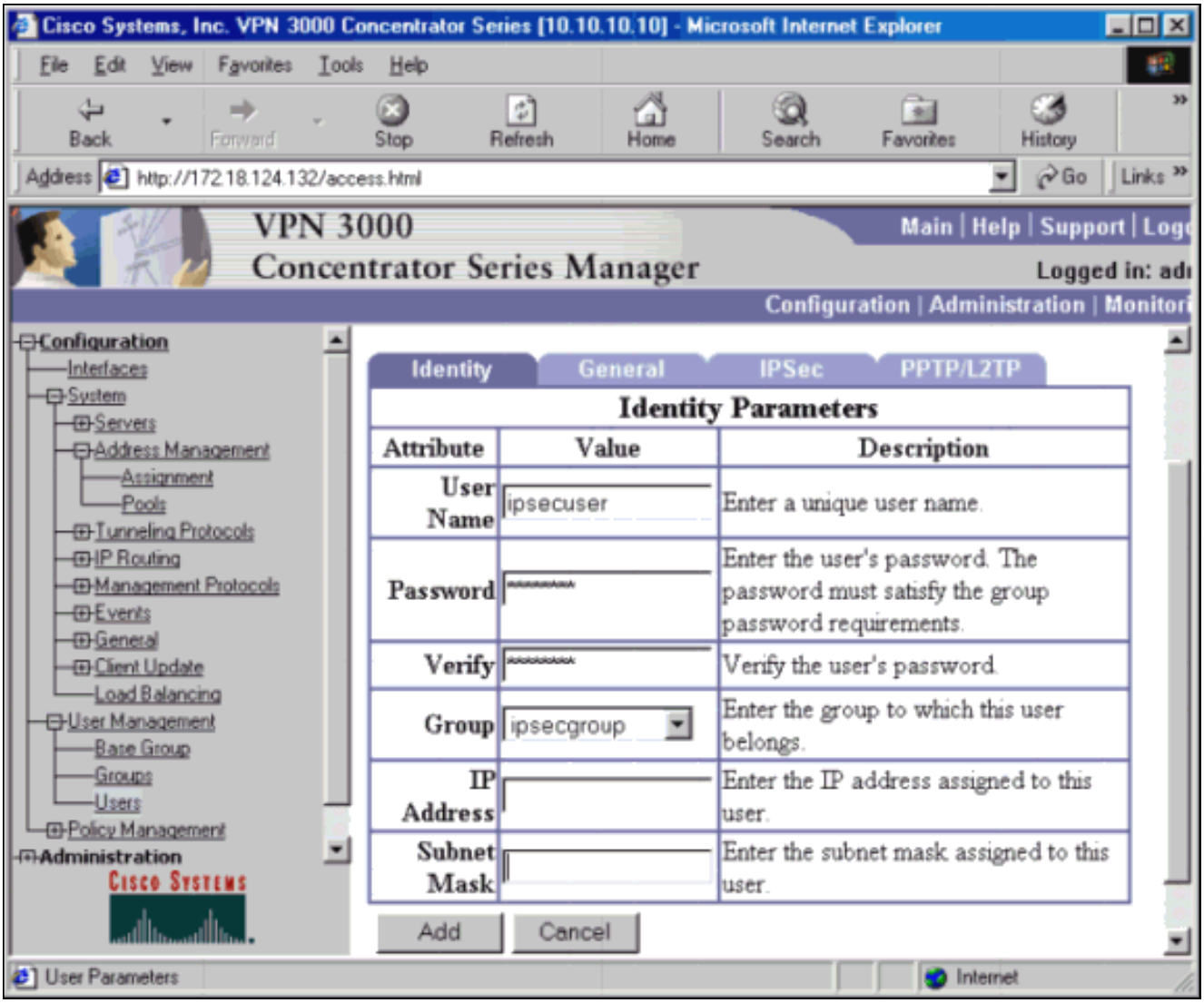
5. في علامة التبويب "عام المجموعات"، حدد **IPSec**.



6. في علامة تبويب Groups IPSec، قم بتعيين المصادقة على **داخلي**.



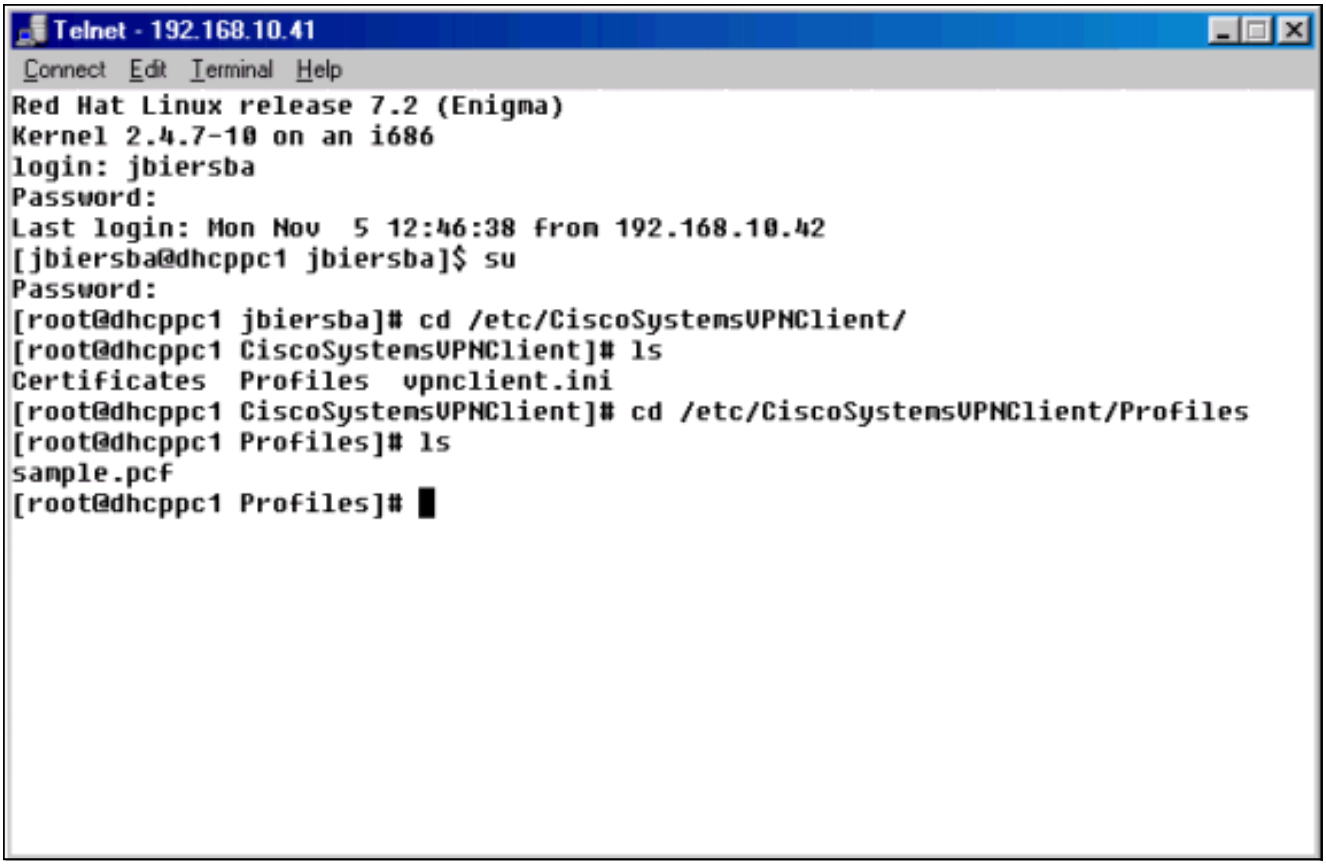
7. انتقل إلى **التكوين > إدارة المستخدم > المستخدمون > إضافة**، وقم بإضافة مستخدم إلى المجموعة المحددة مسبقا. في المثال التالي، المستخدم هو "ipsecuser" مع كلمة المرور "xyz12345" في المجموعة "ipsecgroup".



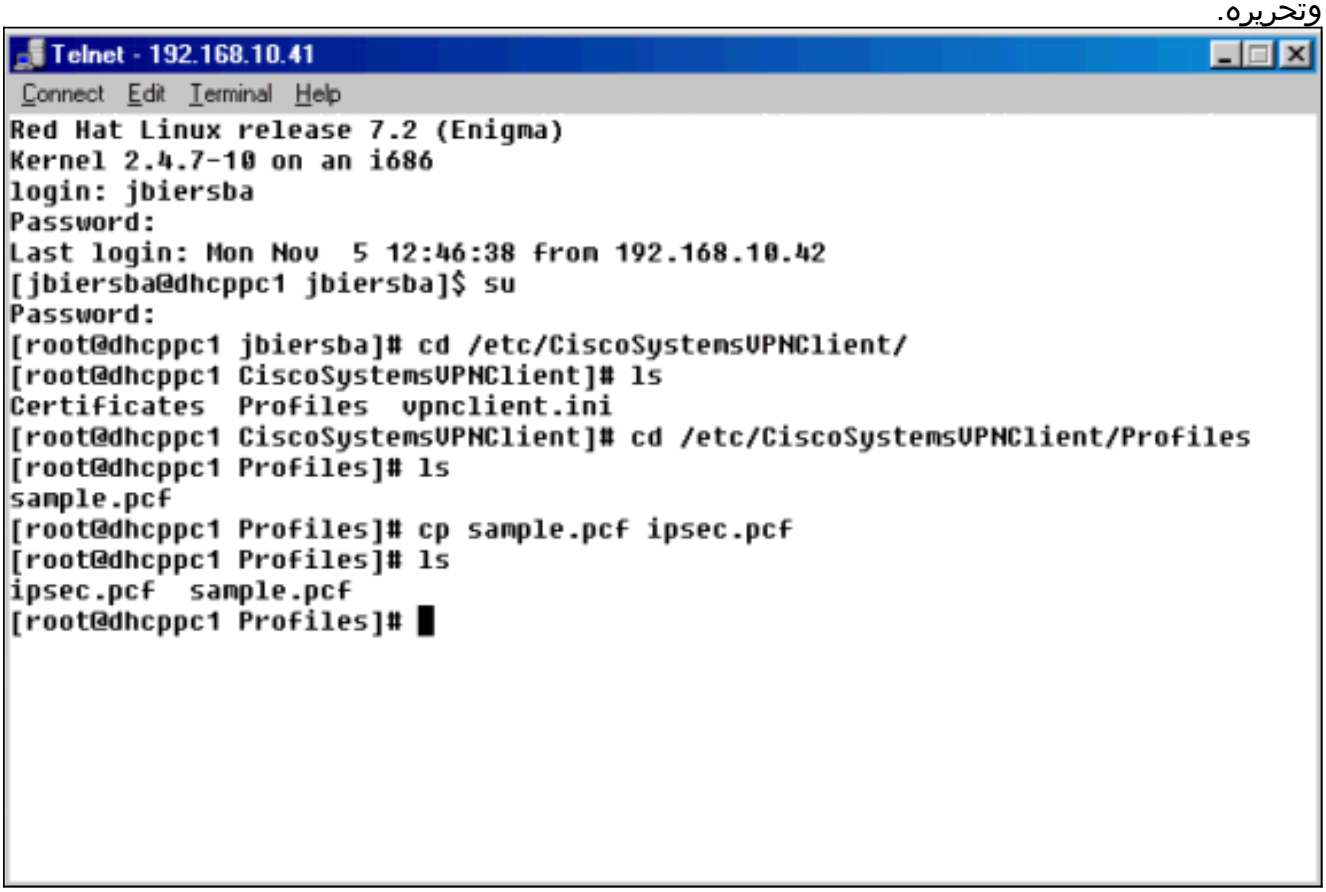
تكوين عميل Linux

اتبع الخطوات التالية:

1. انتقل إلى دليل /etc/CiscoSystemsVPNClient/Profile/ حيث يتم تخزين ملفات تعريف اتصال VPN.

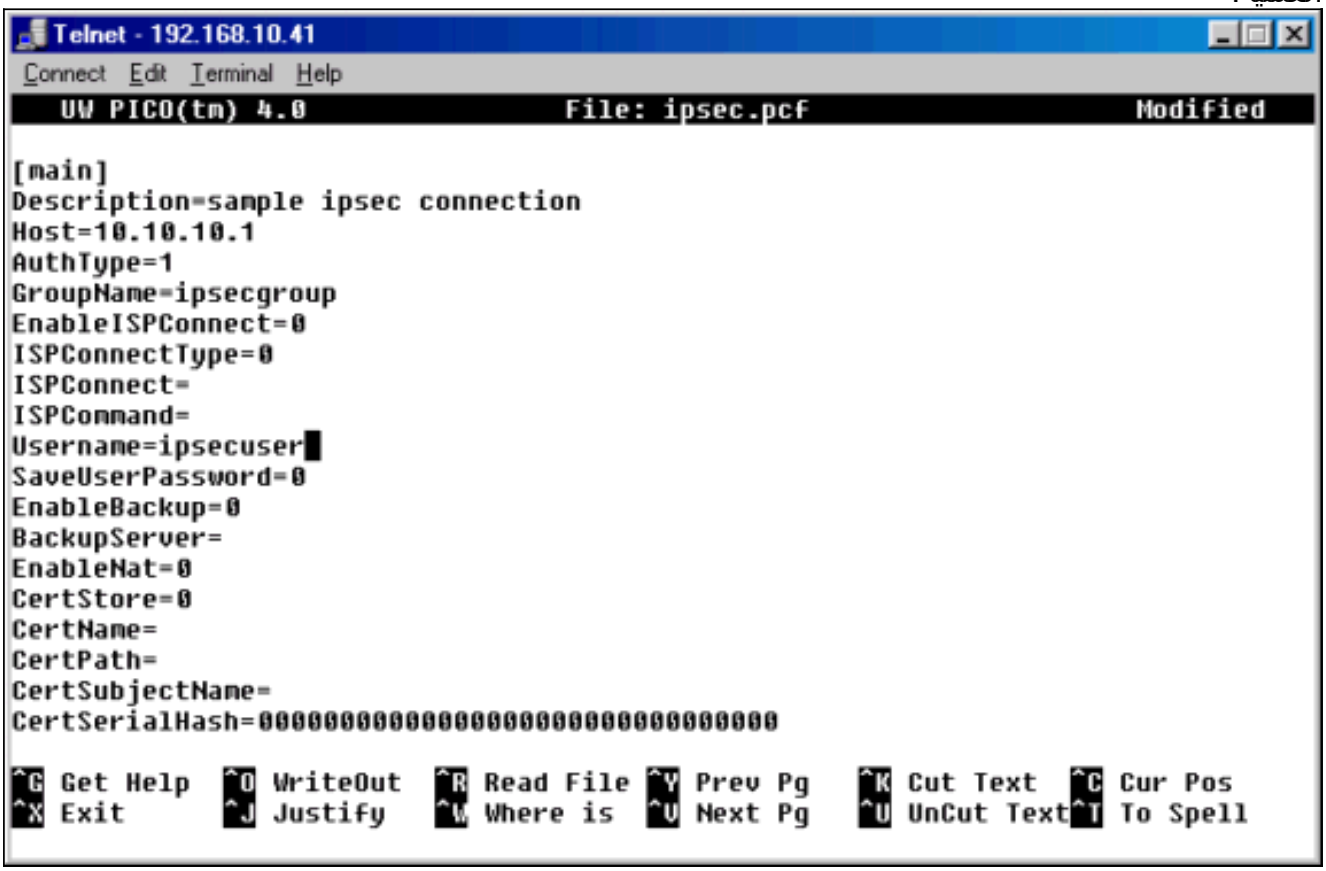


2. افتح ملف تخصيص جديد إما بنسخ ملف التخصيص إلى اسم جديد أو بإنشاء واحد من البداية. في المثال التالي، تم نسخ ملف .pcf العينة، وإعادة تسميته، وتحريره.

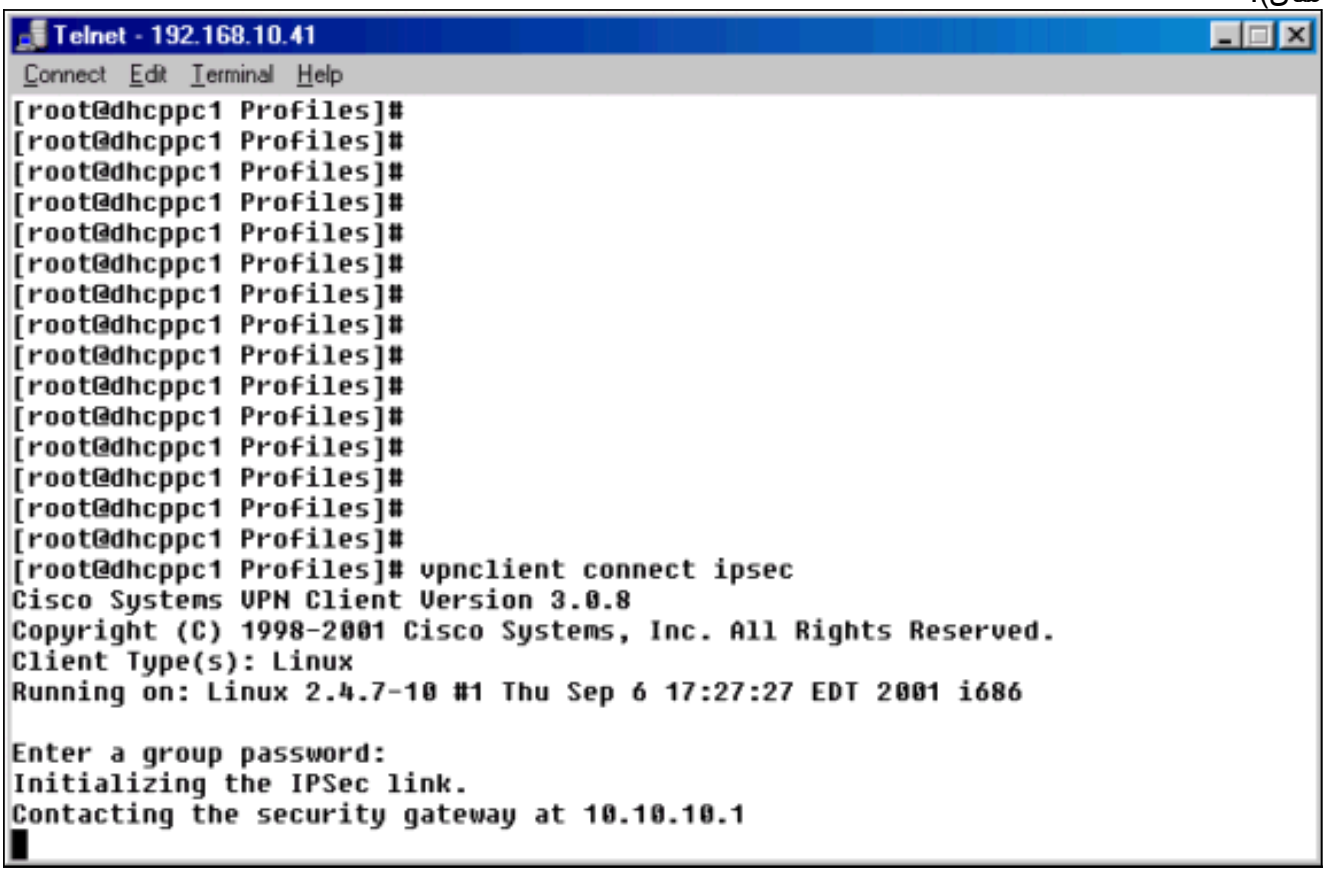


3. قم بتحرير ملف .pcf المسمى حديثا لتضمين المعلومات التالية.وصف جديد لتعريف الاتصالعنوان IP مضيف جديد سيكون عنوان IP الخاص بالواجهة العامة لتركيز VPN 3000اسم مجموعة جديد يلزم مطابقة المجموعة التي تم تكوينها في إعداد مجموعة VPN 3000اسم مستخدم جديد هو نفس اسم المستخدم الذي تم تكوينه على مركز VPN 3000 المتزامن مع مجموعة VPN على المركزثم احفظ الملف وقم بإنهاء

العملية.



4. من موجه الأوامر، أستخدم الأمر **vpnclient connect ipSec** للاتصال بموجه VPN باستخدام ملف IPSec pcf.. ستتم مطالبتك بإدخال كلمة مرور المجموعة. هذا ال نفسه كلمة أن كان شكلت على ال VPN 3000 مركز (كلمة "xyz12345"، في هذا مثال).



5. إذا لم ينجح الاتصال، فالرجاء مراجعة قسم أستكشاف الأخطاء وإصلاحها أدناه.

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

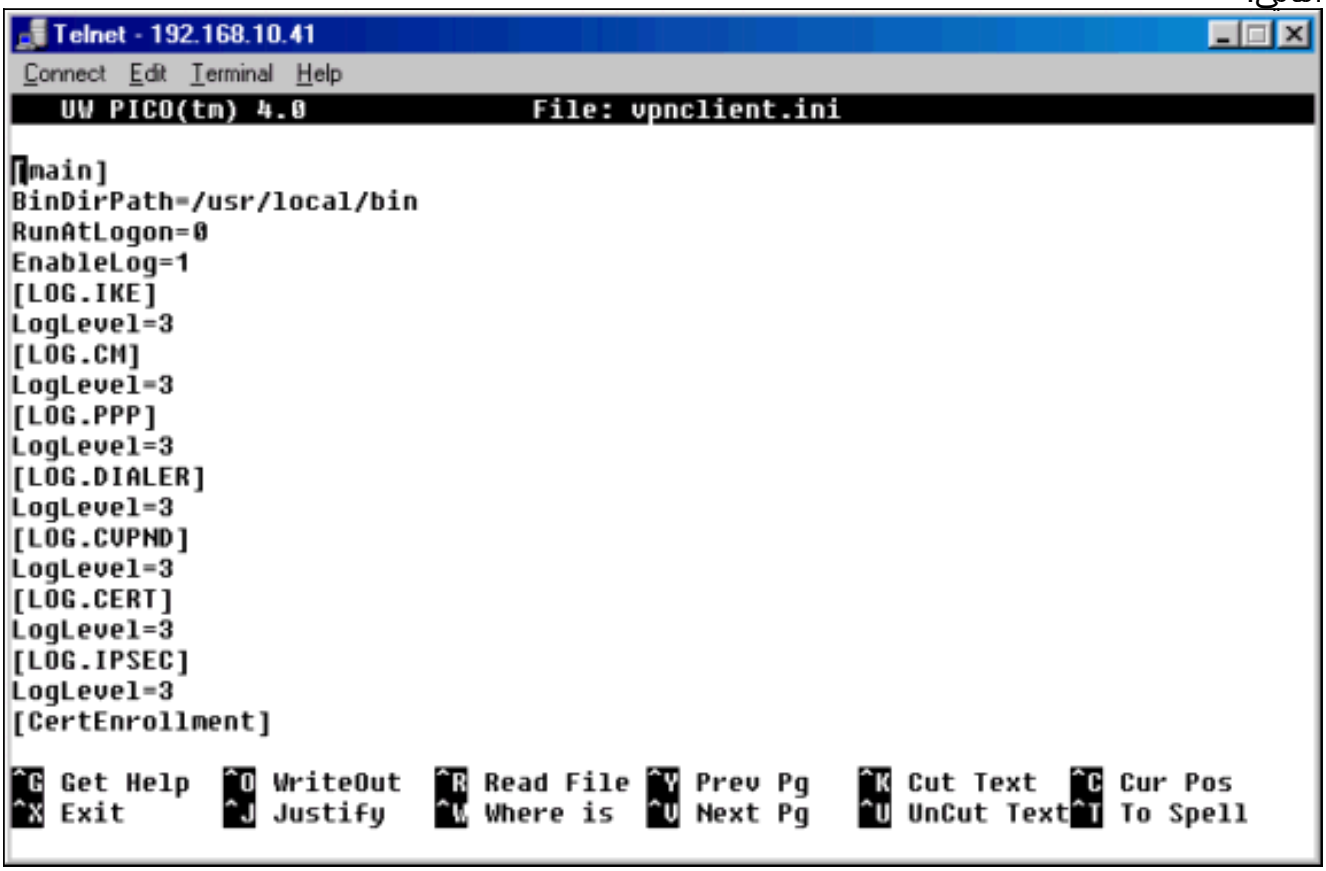
استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

تشغيل تسجيل الدخول إلى عميل VPN

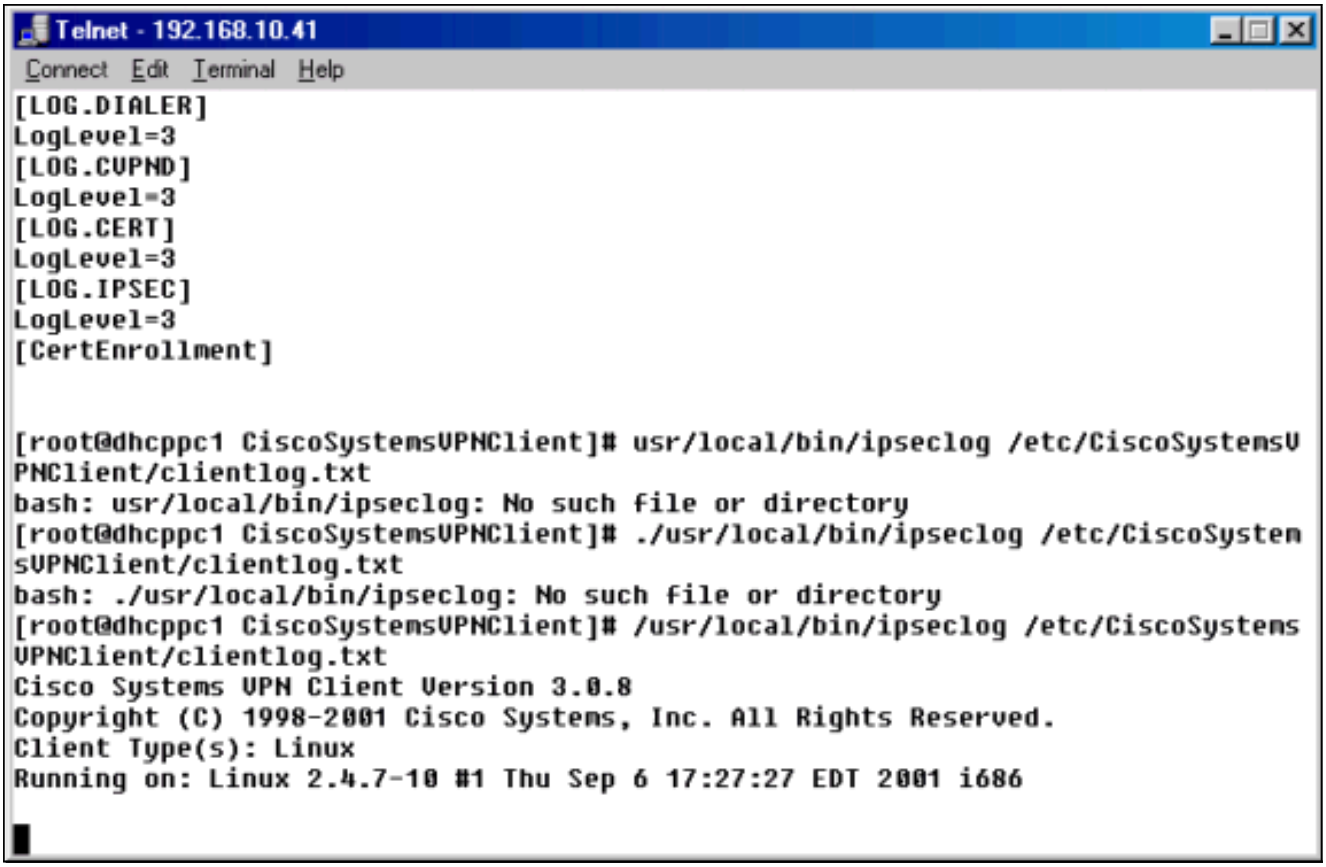
فيما يلي معلومات أستكشاف الأخطاء وإصلاحها المتعلقة بهذا التكوين. اتبع التعليمات التالية لاستكشاف أخطاء عملية التكوين لديك وإصلاحها.

1. قم بإنشاء ملف تعريف عمومي، إذا لم يكن واحدا موجودا بالفعل في الدليل /etc/CiscoSystemsVPNClient/. يجب أن يبدو ملف التعريف العمومي كالمثال التالي.

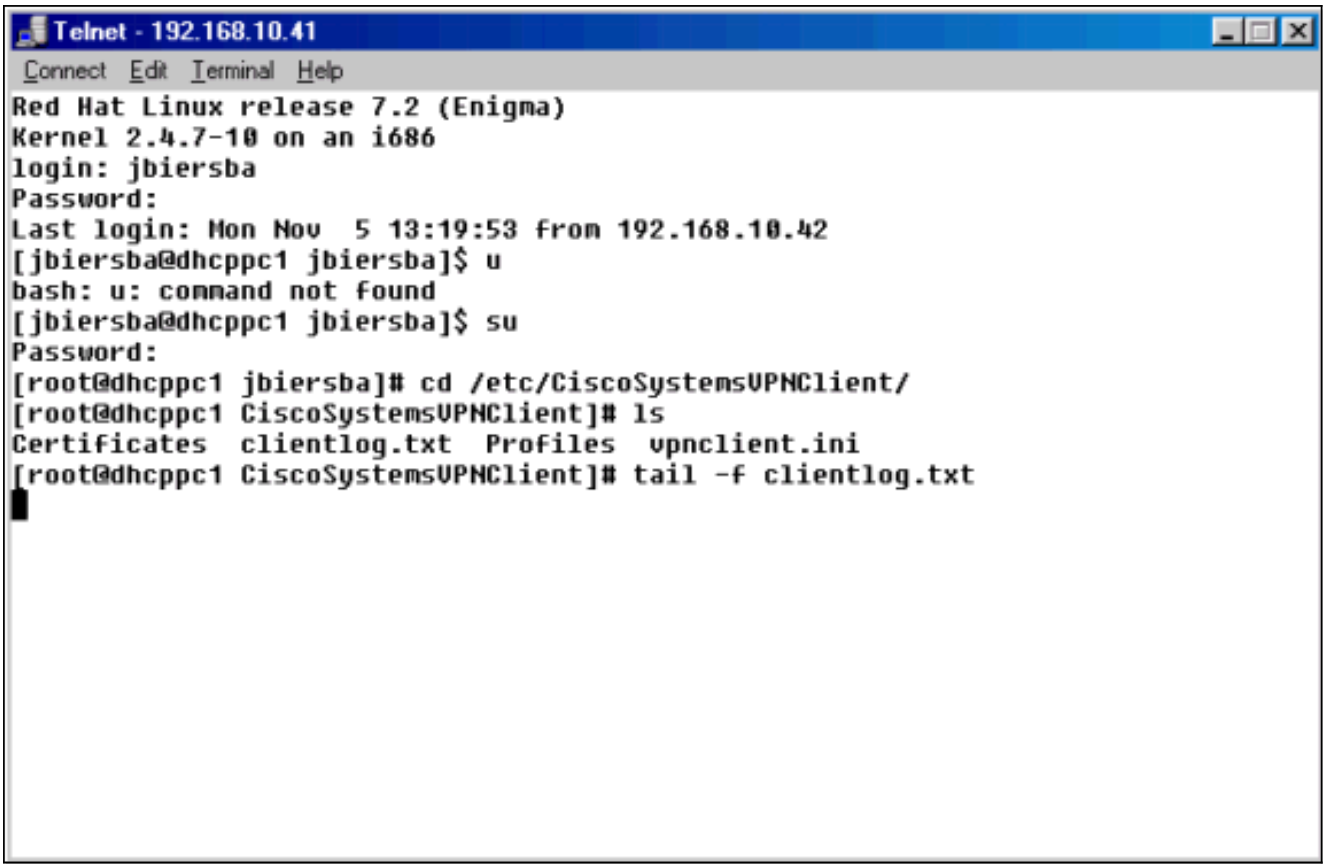


ملاحظة: تأكد من تعيين كل مستوى من مستويات السجل على "3"؛ وسيضمن ذلك تحقيق أعلى مستوى من التسجيل.

2. من موجه الأوامر، أستخدم الأمر **usr/local/bin/ipseclog/** لبدء أداة سجل IPSec المساعدة ونقل المعلومات الموجودة في هذا السجل إلى دليل وملف من إختيارك. في هذا المثال، يسمى الملف clientlog.txt، وهو في دليل /etc/CiscoSystemsVPNClient/:



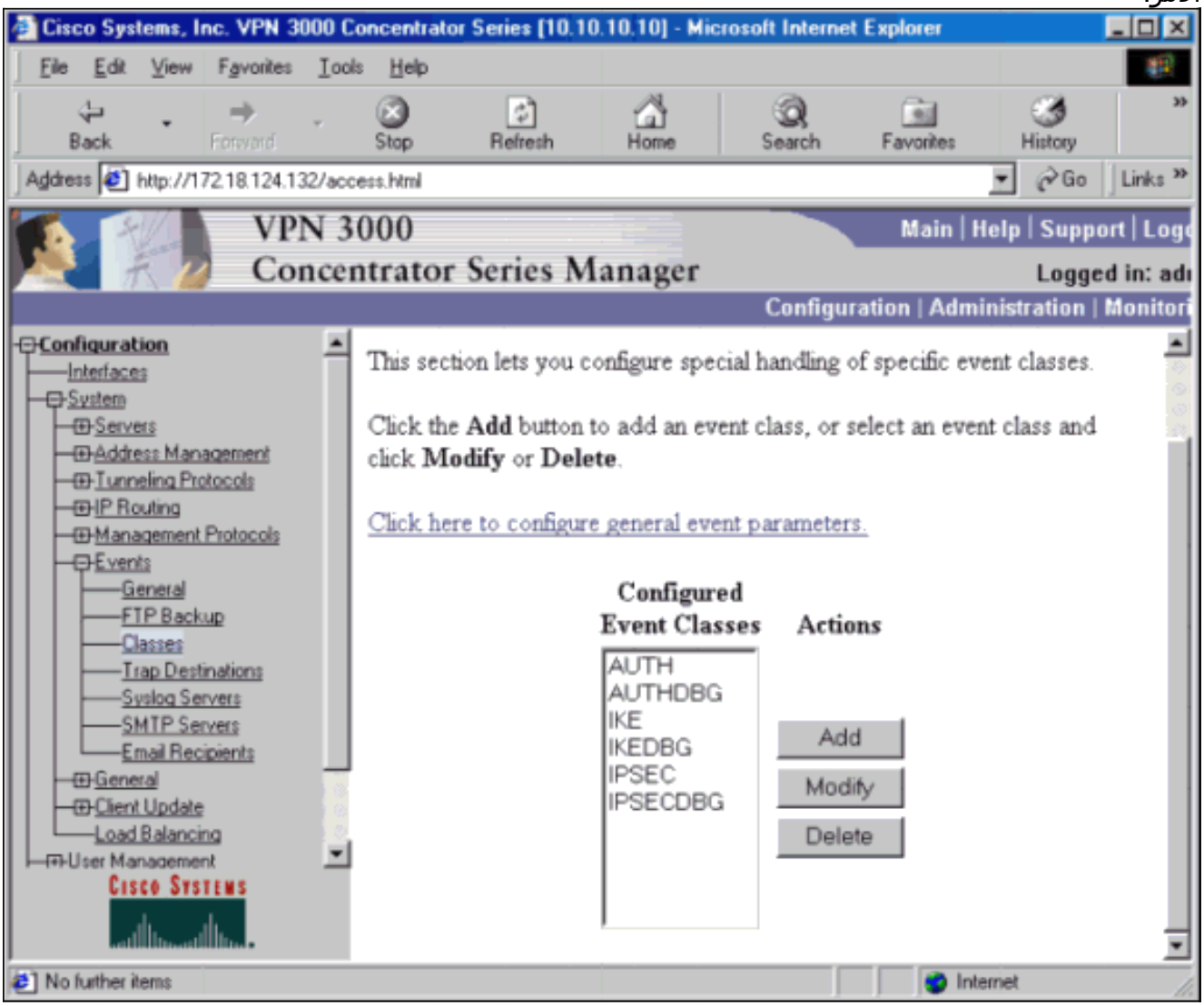
3. في نافذة منفصلة، أستخدم الأمر **tail -f** (لاسم الملف) للحصول على لقطة يتم تحديثها باستمرار لملف clientlog.txt أثناء إتصالك بجمع معلومات تصحيح الأخطاء.



تشغيل التسجيل على مركز VPN 3000

اتبع التعليمات التالية لاستكشاف أخطاء عملية التكوين لديك وإصلاحها.

1. انتقل إلى **التكوين > النظام > الأحداث > الفئات** لتشغيل تصحيح الأخطاء التالي إذا كان هناك حالات فشل في اتصال الأحداث.المصادقة - الخطورة للتسجيل من 1 إلى 13AUTHDBG - الخطورة إلى سجل من 1 إلى 13IKE - الخطورة التي يمكن تسجيلها من 1 إلى 13IKEDBG - الخطورة بالنسبة إلى التسجيل من 1 إلى 13IPSec - الخطورة إلى سجل من 1 إلى 13IPSECDBG - مستوى الخطورة للتسجيل من 1 إلى 13**ملاحظة:** يمكن إضافة Authdecode و iKedecode و IPSECDECODE لاحقا إذا لزم الأمر.



2. يمكنك عرض السجل بالانتقال إلى **المراقبة > سجل أحداث قابل للتصفية**.

تصحيح جيد

- عميل شبكة VPN
- مركز VPN 3000

عميل شبكة VPN

```
Sev=Info/4 CVPND/0x4340000F 11/05/2001 14:02:24.118 1

:Started cvpnd

Cisco Systems VPN Client Version 3.0.8

.Copyright (C) 1998-2001 Cisco Systems, Inc. All Rights Reserved

Client Type(s): Linux

Running on: Linux 2.4.7-10 #1 Thu Sep 6 17:27:27 EDT 2001 i686

Sev=Info/4 IPSEC/0x43700013 11/05/2001 14:02:24.118 2

Delete internal key with SPI=0xcfa58e9f

Sev=Info/4 IPSEC/0x4370000C 11/05/2001 14:02:24.118 3
```

```
                                Key deleted by SPI 0xcfa58e9f
 Sev=Info/4 IPSEC/0x43700013 11/05/2001 14:02:24.118 4
                     Delete internal key with SPI=0x3a21bb45
 Sev=Info/4 IPSEC/0x4370000C 11/05/2001 14:02:24.118 5
                                Key deleted by SPI 0x3a21bb45
 Sev=Info/4 IPSEC/0x43700013 11/05/2001 14:02:24.118 6
                     Delete internal key with SPI=0xc76d7f87
 Sev=Info/4 IPSEC/0x4370000C 11/05/2001 14:02:24.118 7
                                Key deleted by SPI 0xc76d7f87
 Sev=Info/4 IPSEC/0x43700013 11/05/2001 14:02:24.118 8
                     Delete internal key with SPI=0x8fd46a6a
 Sev=Info/4 IPSEC/0x4370000C 11/05/2001 14:02:24.118 9
                                Key deleted by SPI 0x8fd46a6a
Sev=Info/4 IPSEC/0x43700014 11/05/2001 14:02:24.119 10
                                             Deleted all keys
Sev=Info/4 IPSEC/0x43700014 11/05/2001 14:02:24.119 11
                                             Deleted all keys
Sev=Info/4 IPSEC/0x4370000A 11/05/2001 14:02:24.119 12
                           IPSec driver successfully stopped
Sev=Info/4 IPSEC/0x43700014 11/05/2001 14:02:24.119 13
                                             Deleted all keys
Sev=Info/4 IPSEC/0x43700008 11/05/2001 14:02:24.119 14
                           IPSec driver successfully started
Sev=Info/4 IPSEC/0x43700014 11/05/2001 14:02:24.119 15
                                             Deleted all keys
Sev=Info/4 IPSEC/0x4370000D 11/05/2001 14:02:24.119 16
                    (Key(s) deleted by Interface (192.168.10.41
   Sev=Info/4 CM/0x43100002 11/05/2001 14:02:24.960 17
                                      Begin connection process
   Sev=Info/4 CM/0x43100004 11/05/2001 14:02:24.963 18
                         Establish secure connection using Ethernet
   Sev=Info/4 CM/0x43100026 11/05/2001 14:02:24.963 19
```

"Attempt connection with server "rtp-vpn-cluster.cisco.com

Sev=Info/6 IKE/0x4300003B 11/05/2001 14:02:24.980 20

.Attempting to establish a connection with 161.44.127.194

Sev=Debug/7 IKE/0x4300000A 11/05/2001 14:02:25.136 21

.Sending ID me = ID_KEY ciscovpncluster-nat

Sev=Info/4 IKE/0x43000013 11/05/2001 14:02:25.136 22

SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID) to 161.44.127.194

Sev=Decode/11 IKE/0x43000001 11/05/2001 14:02:25.139 23

ISAKMP Header

Initiator COOKIE: ACD9BE3AC57BBE35

Responder COOKIE: 0000000000000000

Next Payload: Security Association

Ver: 10

Exchange Type: Aggressive Mode

(Flags: (none

MessageID: 00000000

Length: 469762048

Payload Security Association

Next Payload: Key Exchange

Reserved: 0000

Payload Length: 308

DOI: IPsec

(Situation:(SIT_IDENTITY_ONLY

Payload Proposal

Next Payload: None

Reserved: 0000

Payload Length: 296

Proposal #: 1

Protocol-Id: PROTO_ISAKMP

SPI Size: 0

of transfroms: 8 #

:SPI

Payload Transform

Next Payload: Transform

Reserved: 0000

Payload Length: 36

Transform #: 1

Transform-Id: KEY_IKE

Reserved2: 0000

Encryption Algorithm: 3DES-CBC

Hash Algorithm: SHA1

Group Description: Group 2

Authentication Method: XAUTHInitPreShared

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Transform

Next Payload: Transform

Reserved: 0000

Payload Length: 36

Transform #: 2

Transform-Id: KEY_IKE

Reserved2: 0000

Encryption Algorithm: 3DES-CBC

Hash Algorithm: MD5

Group Description: Group 2

Authentication Method: XAUTHInitPreShared

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Transform

Next Payload: Transform

Reserved: 0000

Payload Length: 36

Transform #: 3

Transform-Id: KEY_IKE

Reserved2: 0000

Encryption Algorithm: 3DES-CBC

Hash Algorithm: SHA1

Group Description: Group 2

Authentication Method: Preshared key

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Transform

Next Payload: Transform

Reserved: 0000

Payload Length: 36

Transform #: 4

Transform-Id: KEY_IKE

Reserved2: 0000

Encryption Algorithm: 3DES-CBC

Hash Algorithm: MD5

Group Description: Group 2

Authentication Method: Preshared key

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Transform

Next Payload: Transform

Reserved: 0000

Payload Length: 36

Transform #: 5

Transform-Id: KEY_IKE

Reserved2: 0000

Encryption Algorithm: DES-CBC

Hash Algorithm: SHA1

Group Description: Group 2

Authentication Method: XAUTHInitPreShared

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Transform

Next Payload: Transform

Reserved: 0000

Payload Length: 36

Transform #: 6

Transform-Id: KEY_IKE

Reserved2: 0000

Encryption Algorithm: DES-CBC

Hash Algorithm: MD5

Group Description: Group 2

Authentication Method: XAUTHInitPreShared

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Transform

Next Payload: Transform

Reserved: 0000

Payload Length: 36

Transform #: 7

Transform-Id: KEY_IKE

Reserved2: 0000

Encryption Algorithm: DES-CBC

Hash Algorithm: SHA1

Group Description: Group 2

Authentication Method: Preshared key

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 36

Transform #: 8

Transform-Id: KEY_IKE

Reserved2: 0000

Encryption Algorithm: DES-CBC

Hash Algorithm: MD5

Group Description: Group 2

Authentication Method: Preshared key

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Key Exchange

Next Payload: Nonce

Reserved: 0000

Payload Length: 132

Data: 14B9E06FB0742252C9CDA9C0E1045036FCE13E88E84A868EE895743
287DBD865FF938F144197B85865F39D6ED5BF7B16CBE49EA64DF07CE6840D
4105D800CE463CB310BF85D145CF63659CD9F7403CF486C27C37D086A4A57
5AE655F547DF9FF1DAC0F5ECE37FA5D91DC58F3B1C3331D78C6D711C316A1
70A8515219147FB0C405000018

Payload Nonce

Next Payload: Identification

Reserved: 0000

Payload Length: 24

Data: 18ADE217264969EBC698E5742FDAE5A6F1E8555F0D00001B

Payload Identification

Next Payload: Vendor ID

Reserved: 0000

Payload Length: 27

ID Type: ID_KEY_ID

Protocol ID (UDP/TCP, etc...): 17

Port: 500

ID Data: ciscovpncluster-nat

Payload Vendor ID

Next Payload: Vendor ID

Reserved: 0000

Payload Length: 12

Data (In Hex): 09002689DFD6B712

Payload Vendor ID

Next Payload: Vendor ID

Reserved: 0000

Payload Length: 20

Data (In Hex): AFCAD71368A1F1C96B8696FC77570100

Payload Vendor ID

Next Payload: None

Reserved: 0000

Payload Length: 20

Data (In Hex): 12F5F28C457168A9702D9FE274CC0100

Sev=Info/4 IPSEC/0x43700014 11/05/2001 14:02:25.140 24

Deleted all keys

Sev=Info/4 IPSEC/0x4370000D 11/05/2001 14:02:25.140 25

(Key(s) deleted by Interface (192.168.10.41

Sev=Info/5 IKE/0x4300002F 11/05/2001 14:02:25.341 26

Received ISAKMP packet: peer = 161.44.127.194

Sev=Decode/11 IKE/0x43000001 11/05/2001 14:02:25.343 27

ISAKMP Header

Initiator COOKIE: ACD9BE3AC57BBE35

Responder COOKIE: F8D106BDD3A6236D

Next Payload: Security Association

Ver: 10

Exchange Type: Aggressive Mode

(Flags: (none

MessageID: 00000000

Length: 344

Payload Security Association

Next Payload: Key Exchange

Reserved: 0000

Payload Length: 56

DOI: IPsec

(Situation:(SIT_IDENTITY_ONLY

Payload Proposal

Next Payload: None

Reserved: 0000

Payload Length: 44

Proposal #: 1

Protocol-Id: PROTO_ISAKMP

SPI Size: 0

of transfroms: 1 #

:SPI

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 36

Transform #: 2

Transform-Id: KEY_IKE

Reserved2: 0000

Encryption Algorithm: 3DES-CBC

Hash Algorithm: MD5

Group Description: Group 2

Authentication Method: XAUTHInitPreShared

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Key Exchange

Next Payload: Nonce

Reserved: 0000

Payload Length: 132

Data: 0F428F30FAD939D04BB301934BD24252585691E9A5AA30DF3
E67B04A2BAF010C5B0F890D422AD68592AA11F0AD8DCA20766AF42C
F93850EC73526CFE91B953CF6A5B38A051CB6D7673A6F69E15ACE9D
7793FFC2A89B88135EA5DE187961E64869787008EFCBE1BEF40C34F
AE1A278F1BEE8DF3BA873DCDA9A33DC14FBE59D77605000018

Payload Nonce

Next Payload: Identification

Reserved: 0000

Payload Length: 24

Data: B466B5297839DDB8D45177EE87DABC1463EB8D4C0800000C

Payload Identification

Next Payload: Hash

Reserved: 0000

Payload Length: 12

ID Type: IPv4 Address

Protocol ID (UDP/TCP, etc...): 17

Port: 500

ID Data: 161.44.127.194

Payload Hash

Next Payload: Vendor ID

Reserved: 0000

Payload Length: 20

Data: E1F2B6C63282B7091A0DA4F1F9C056E30D000014

Payload Vendor ID

Next Payload: Vendor ID

Reserved: 0000

Payload Length: 20

Data (In Hex): 12F5F28C457168A9702D9FE274CC0100

Payload Vendor ID

Next Payload: Vendor ID

Reserved: 0000

Payload Length: 12

Data (In Hex): 09002689DFD6B712

Payload Vendor ID

Next Payload: Vendor ID

Reserved: 0000

Payload Length: 20

Data (In Hex): AFCAD71368A1F1C96B8696FC77570100

Payload Vendor ID

Next Payload: None

Reserved: 0000

Payload Length: 20

Data (In Hex): 1F07F70EAA6514D3B0FA96542A500300

Sev=Info/4 IKE/0x43000014 11/05/2001 14:02:25.344 28

,RECEIVING <<< ISAKMP OAK AG (SA, KE, NON, ID, HASH, VID
VID, VID, VID) from 161.44.127.194

Sev=Info/5 IKE/0x43000059 11/05/2001 14:02:25.344 29

Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100

Sev=Info/5 IKE/0x43000001 11/05/2001 14:02:25.344 30

Peer is a Cisco-Unity compliant peer

Sev=Info/5 IKE/0x43000059 11/05/2001 14:02:25.344 31

Vendor ID payload = 09002689DFD6B712

Sev=Info/5 IKE/0x43000059 11/05/2001 14:02:25.344 32

Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100

Sev=Info/5 IKE/0x43000001 11/05/2001 14:02:25.344 33

Peer supports DPD

Sev=Info/5 IKE/0x43000059 11/05/2001 14:02:25.344 34

Vendor ID payload = 1F07F70EAA6514D3B0FA96542A500300

Sev=Info/4 IKE/0x43000013 11/05/2001 14:02:25.480 35

(SENDING >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT
to 161.44.127.194

Sev=Decode/11 IKE/0x43000001 11/05/2001 14:02:25.483 36

ISAKMP Header

Initiator COOKIE: ACD9BE3AC57BBE35

Responder COOKIE: F8D106BDD3A6236D

Next Payload: Hash

Ver: 10

Exchange Type: Aggressive Mode

(Flags: (Encryption

MessageID: 00000000

Length: 469762048

Payload Hash

Next Payload: Notification

Reserved: 0000

Payload Length: 20

Data: CFCFC21977456B8B6BA6D39AB4EB14B20000001C

Payload Notification

Next Payload: None

Reserved: 0000

Payload Length: 28

DOI: IPsec

Protocol-ID: PROTO_ISAKMP

Spi Size: 16

Notify Type: STATUS_INITIAL_CONTACT

SPI: ACD9BE3AC57BBE35F8D106BDD3A6236D

:Data

Sev=Info/5 IKE/0x4300002F 11/05/2001 14:02:25.524 37

Received ISAKMP packet: peer = 161.44.127.194

Sev=Debug/7 IKE/0x43000022 11/05/2001 14:02:25.524 38

Crypto READY becoming ACTIVE

Sev=Decode/11 IKE/0x43000001 11/05/2001 14:02:25.527 39

ISAKMP Header

Initiator COOKIE: ACD9BE3AC57BBE35

Responder COOKIE: F8D106BDD3A6236D

Next Payload: Hash

Ver: 10

Exchange Type: Informational

(Flags: (Encryption

MessageID: 9A429435

Length: 84

Payload Hash

Next Payload: Notification

Reserved: 0000

Payload Length: 20

Data: 09ED923D74F93C252C056B96F374E80900000020

Payload Notification

Next Payload: None

Reserved: 0000

Payload Length: 32

DOI: IPsec

Protocol-ID: PROTO_ISAKMP

Spi Size: 16

Notify Type: NOTIFY_STATUS_LOAD_BALALANCE

SPI: ACD9BE3AC57BBE35F8D106BDD3A6236D

Data: A12C7FC4

Sev=Info/4 IKE/0x43000014 11/05/2001 14:02:25.527 40

(RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:LOAD_BALANCE
from 161.44.127.194

Sev=Info/4 CM/0x4310001B 11/05/2001 14:02:25.527 41

Received alternative server address "161.44.127.196" from
primary server

Sev=Debug/8 IKE/0x4300004C 11/05/2001 14:02:25.527 42

Stopping DPD timer for IKE SA* 0817FC98

Sev=Info/4 IKE/0x43000013 11/05/2001 14:02:25.528 43

SENDING >>> ISAKMP OAK INFO *(HASH, DEL) to 161.44.127.194

Sev=Decode/11 IKE/0x43000001 11/05/2001 14:02:25.530 44

ISAKMP Header

Initiator COOKIE: ACD9BE3AC57BBE35

Responder COOKIE: F8D106BDD3A6236D

Next Payload: Hash

Ver: 10

Exchange Type: Informational

(Flags: (Encryption

MessageID: D3B8CE2C

Length: 469762048

Payload Hash

Next Payload: Delete

Reserved: 0000

Payload Length: 20

Data: D1461180C869DA6D6A7BDE0A34CE7D030000001C

Payload Delete

Next Payload: None

Reserved: 0000

Payload Length: 28

DOI: Isakmp

Protocol-ID: PROTO_ISAKMP

Spi Size: 16

of SPIs: 1 #

SPI (Hex dump): ACD9BE3AC57BBE35F8D106BDD3A6236D

Sev=Info/4 CM/0x43100014 11/05/2001 14:02:25.531 45

Unable to establish Phase 1 SA with server "rtp-vpn-cluster.cisco.com" because of "DEL_REASON_LOAD_BALANCING"

Sev=Info/4 CM/0x43100010 11/05/2001 14:02:25.531 46

Try alternative server "161.44.127.196" given by the primary server

Sev=Info/4 CM/0x43100026 11/05/2001 14:02:25.531 47

"Attempt connection with server "161.44.127.196

Sev=Info/6 IKE/0x4300003B 11/05/2001 14:02:25.531 48

.Attempting to establish a connection with 161.44.127.196

Sev=Debug/7 IKE/0x4300000A 11/05/2001 14:02:25.678 49

.Sending ID me = ID_KEY ciscovpncluster-nat

Sev=Info/4 IKE/0x43000013 11/05/2001 14:02:25.678 50

(SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID to 161.44.127.196

Sev=Decode/11 IKE/0x43000001 11/05/2001 14:02:25.681 51

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 0000000000000000

Next Payload: Security Association

Ver: 10

Exchange Type: Aggressive Mode

(Flags: (none

MessageID: 00000000

Length: 469762048

Payload Security Association

Next Payload: Key Exchange

Reserved: 0000

Payload Length: 308

DOI: IPsec

(Situation:(SIT_IDENTITY_ONLY

Payload Proposal

Next Payload: None

Reserved: 0000

Payload Length: 296

Proposal #: 1

Protocol-Id: PROTO_ISAKMP

SPI Size: 0

of transfroms: 8 #

:SPI

Payload Transform

Next Payload: Transform

Reserved: 0000

Payload Length: 36

Transform #: 1

Transform-Id: KEY_IKE

Reserved2: 0000

Encryption Algorithm: 3DES-CBC

Hash Algorithm: SHA1

Group Description: Group 2

Authentication Method: XAUTHInitPreShared

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Transform

Next Payload: Transform

Reserved: 0000

Payload Length: 36

Transform #: 2

Transform-Id: KEY_IKE

Reserved2: 0000

Encryption Algorithm: 3DES-CBC

Hash Algorithm: MD5

Group Description: Group 2

Authentication Method: XAUTHInitPreShared

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Transform

Next Payload: Transform

Reserved: 0000

Payload Length: 36

Transform #: 3

Transform-Id: KEY_IKE

Reserved2: 0000

Encryption Algorithm: 3DES-CBC

Hash Algorithm: SHA1

Group Description: Group 2

Authentication Method: Preshared key

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Transform

Next Payload: Transform

Reserved: 0000

Payload Length: 36

Transform #: 4

Transform-Id: KEY_IKE

Reserved2: 0000

Encryption Algorithm: 3DES-CBC

Hash Algorithm: MD5

Group Description: Group 2

Authentication Method: Preshared key

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Transform

Next Payload: Transform

Reserved: 0000

Payload Length: 36

Transform #: 5

Transform-Id: KEY_IKE

Reserved2: 0000

Encryption Algorithm: DES-CBC

Hash Algorithm: SHA1

Group Description: Group 2

Authentication Method: XAUTHInitPreShared

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Transform

Next Payload: Transform

Reserved: 0000

Payload Length: 36

Transform #: 6

Transform-Id: KEY_IKE

Reserved2: 0000

Encryption Algorithm: DES-CBC

Hash Algorithm: MD5

Group Description: Group 2

Authentication Method: XAUTHInitPreShared

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Transform

Next Payload: Transform

Reserved: 0000

Payload Length: 36

Transform #: 7

Transform-Id: KEY_IKE

Reserved2: 0000

Encryption Algorithm: DES-CBC

Hash Algorithm: SHA1

Group Description: Group 2

Authentication Method: Preshared key

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 36

Transform #: 8

Transform-Id: KEY_IKE

Reserved2: 0000

Encryption Algorithm: DES-CBC

Hash Algorithm: MD5

Group Description: Group 2

Authentication Method: Preshared key

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Key Exchange

Next Payload: Nonce

Reserved: 0000

Payload Length: 132

Data: 7F445582B28E0DA53D4D7C42E50582503B5771C46C357F98
4DCB7A9549F5F6789E05016095F4FEFD3C2B1206CBCE63681AF2D5
5BEED5524D989636C22523665E58F7D338DFD7D7F838CF4A0514C7
F3F87BBCB053E257D08B8A2AD988AABB63B692852FFE4E550C4020
A0A3058170F6CA53C3C2BEC27045FD8B7C724E2ED1BD3405000018

Payload Nonce

Next Payload: Identification

Reserved: 0000

Payload Length: 24

Data: 5A57FF12D4D74824EB0103E3E2D7C3A5403BDA0F0D00001B

Payload Identification

Next Payload: Vendor ID

Reserved: 0000

Payload Length: 27

ID Type: ID_KEY_ID

Protocol ID (UDP/TCP, etc...): 17

Port: 500

ID Data: ciscovpncluster-nat

Payload Vendor ID

Next Payload: Vendor ID

Reserved: 0000

Payload Length: 12

Data (In Hex): 09002689DFD6B712

Payload Vendor ID

Next Payload: Vendor ID

Reserved: 0000

Payload Length: 20

Data (In Hex): AFCAD71368A1F1C96B8696FC77570100

Payload Vendor ID

Next Payload: None

Reserved: 0000

Payload Length: 20

Data (In Hex): 12F5F28C457168A9702D9FE274CC0100

Sev=Debug/8 IKE/0x4300004C 11/05/2001 14:02:25.682 52

Stopping DPD timer for IKE SA* 0817FC98

Sev=Info/5 IKE/0x4300002F 11/05/2001 14:02:25.682 53

Received ISAKMP packet: peer = 161.44.127.194

Sev=Warning/2 IKE/0xC3000080 11/05/2001 14:02:25.682 54

Received an IKE packet from someone other than the
.Concentrator that we are currently connected to... discarding packet

Sev=Info/5 IKE/0x4300002F 11/05/2001 14:02:25.883 55

Received ISAKMP packet: peer = 161.44.127.196

Sev=Decode/11 IKE/0x43000001 11/05/2001 14:02:25.886 56

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Security Association

Ver: 10

Exchange Type: Aggressive Mode

(Flags: (none

MessageID: 00000000

Length: 344

Payload Security Association

Next Payload: Key Exchange

Reserved: 0000

Payload Length: 56

DOI: IPsec

(Situation:(SIT_IDENTITY_ONLY

Payload Proposal

Next Payload: None

Reserved: 0000

Payload Length: 44

Proposal #: 1

Protocol-Id: PROTO_ISAKMP

SPI Size: 0

of transfroms: 1 #

:SPI

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 36

Transform #: 2

Transform-Id: KEY_IKE

Reserved2: 0000

Encryption Algorithm: 3DES-CBC

Hash Algorithm: MD5

Group Description: Group 2

Authentication Method: XAUTHInitPreShared

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Key Exchange

Next Payload: Nonce

Reserved: 0000

Payload Length: 132

Data: 71A75D31C3251028E8B893C8268A3CBF626ADCC4BE8A550F
C2EFFAD981C25B68145B42F554E505CD90C1309F46335EF4E1E064
9A54C5D1E0496E5A169690B1FAA8AFE69271C09D9189EFE993CBD5
BECB9FF304F00BA8CD6509551FC7D5BB3AB97FF3464E4E29400232
88BBF1E698C3E0C58BCAD5D69E881F47981CCA00E221DA05000018

Payload Nonce

Next Payload: Identification

Reserved: 0000

Payload Length: 24

Data: 392387EED0F758D660D57DF42F937AD1EE2A80AF0800000C

Payload Identification

Next Payload: Hash

Reserved: 0000

Payload Length: 12

ID Type: IPv4 Address

Protocol ID (UDP/TCP, etc...): 17

Port: 500

ID Data: 161.44.127.196

Payload Hash

Next Payload: Vendor ID

Reserved: 0000

Payload Length: 20

Data: FD17C6600A11AB661CF746CA2B9BB0CE0D000014

Payload Vendor ID

Next Payload: Vendor ID

Reserved: 0000

Payload Length: 20

Data (In Hex): 12F5F28C457168A9702D9FE274CC0100

Payload Vendor ID

Next Payload: Vendor ID

Reserved: 0000

Payload Length: 12

Data (In Hex): 09002689DFD6B712

Payload Vendor ID

Next Payload: Vendor ID

Reserved: 0000

Payload Length: 20

Data (In Hex): AFCAD71368A1F1C96B8696FC77570100

Payload Vendor ID

Next Payload: None

Reserved: 0000

Payload Length: 20

Data (In Hex): 1F07F70EAA6514D3B0FA96542A500300

Sev=Info/4 IKE/0x43000014 11/05/2001 14:02:25.887 57

,RECEIVING <<< ISAKMP OAK AG (SA, KE, NON, ID, HASH, VID
VID, VID, VID) from 161.44.127.196

Sev=Info/5 IKE/0x43000059 11/05/2001 14:02:25.887 58

Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100

Sev=Info/5 IKE/0x43000001 11/05/2001 14:02:25.887 59

Peer is a Cisco-Unity compliant peer

Sev=Info/5 IKE/0x43000059 11/05/2001 14:02:25.887 60

Vendor ID payload = 09002689DFD6B712

Sev=Info/5 IKE/0x43000059 11/05/2001 14:02:25.887 61

Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100

Sev=Info/5 IKE/0x43000001 11/05/2001 14:02:25.887 62

Peer supports DPD

Sev=Info/5 IKE/0x43000059 11/05/2001 14:02:25.887 63

Vendor ID payload = 1F07F70EAA6514D3B0FA96542A500300

Sev=Info/4 IKE/0x43000013 11/05/2001 14:02:26.036 64

(SENDING >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT
to 161.44.127.196

Sev=Decode/11 IKE/0x43000001 11/05/2001 14:02:26.039 65

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Aggressive Mode

(Flags: (Encryption

MessageID: 00000000

Length: 469762048

Payload Hash

Next Payload: Notification

Reserved: 0000

Payload Length: 20

Data: 09E5321B10682CCF4C87EDE7EC41E3810000001C

Payload Notification

Next Payload: None

Reserved: 0000

Payload Length: 28

DOI: IPsec

Protocol-ID: PROTO_ISAKMP

Spi Size: 16

Notify Type: STATUS_INITIAL_CONTACT

SPI: DACB1B32139742E7630E88F067C1B0B5

:Data

Sev=Info/5 IKE/0x4300002F 11/05/2001 14:02:26.081 66

Received ISAKMP packet: peer = 161.44.127.196

Sev=Debug/7 IKE/0x43000022 11/05/2001 14:02:26.081 67

Crypto READY becoming ACTIVE

Sev=Decode/11 IKE/0x43000001 11/05/2001 14:02:26.084 68

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Transaction

(Flags: (Encryption

MessageID: D16C4008

Length: 100

Payload Hash

Next Payload: Attributes

Reserved: 0000

Payload Length: 20

Data: EFB8FABB63311D72DDB7F15A809215B700000034

Payload Attributes

Next Payload: None

Reserved: 0000

Payload Length: 52

type: ISAKMP_CFG_REQUEST

Reserved: 00

Identifier: 0000

XAUTH Type: RADIUS-CHAP

(XAUTH User Name: (empty

(XAUTH User Password: (empty

(XAUTH Message: (data not displayed

Sev=Info/4 IKE/0x43000014 11/05/2001 14:02:26.084 69

RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 161.44.127.196

Sev=Info/4 CM/0x43100015 11/05/2001 14:02:26.084 70

Launch xAuth application

Sev=Info/4 IPSEC/0x43700012 11/05/2001 14:02:27.098 71

Delete all keys associated with peer 161.44.127.194

Sev=Info/4 IPSEC/0x43700014 11/05/2001 14:02:27.098 72

Deleted all keys

Sev=Info/4 IPSEC/0x4370000D 11/05/2001 14:02:27.098 73

(Key(s) deleted by Interface (192.168.10.41

Sev=Info/4 CM/0x43100017 11/05/2001 14:02:42.971 74

xAuth application returned

Sev=Info/4 IKE/0x43000013 11/05/2001 14:02:42.971 75

SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 161.44.127.196

Sev=Decode/11 IKE/0x43000001 11/05/2001 14:02:42.974 76

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Transaction

(Flags: (Encryption

MessageID: 08406CD1

Length: 469762048

Payload Hash

Next Payload: Attributes

Reserved: 0000

Payload Length: 20

Data: 0E26F47ABBA0AF052EA3B9DC6E34C9B300000024

Payload Attributes

Next Payload: None

Reserved: 0000

Payload Length: 36

type: ISAKMP_CFG_REPLY

Reserved: 00

Identifier: 0000

XAUTH Type: RADIUS-CHAP

(XAUTH User Name: (data not displayed

(XAUTH User Password: (data not displayed

Sev=Info/5 IKE/0x4300002F 11/05/2001 14:02:43.819 77

Received ISAKMP packet: peer = 161.44.127.196

Sev=Decode/11 IKE/0x43000001 11/05/2001 14:02:43.822 78

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Transaction

(Flags: (Encryption

MessageID: 4D49FD67

Length: 60

Payload Hash

Next Payload: Attributes

Reserved: 0000

Payload Length: 20

Data: 20516C85949FEB6061853707A36B730D0000000C

Payload Attributes

Next Payload: None

Reserved: 0000

Payload Length: 12

type: ISAKMP_CFG_SET

Reserved: 00

Identifier: 0000

XAUTH Status: Pass

Sev=Info/4 IKE/0x43000014 11/05/2001 14:02:43.822 79

RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 161.44.127.196

Sev=Info/4 CM/0x4310000E 11/05/2001 14:02:43.822 80

Established Phase 1 SA. 1 Phase 1 SA in the system

Sev=Info/4 IKE/0x43000013 11/05/2001 14:02:43.825 81

SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 161.44.127.196

Sev=Decode/11 IKE/0x43000001 11/05/2001 14:02:43.828 82

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Transaction

(Flags: (Encryption

MessageID: 67FD494D

Length: 469762048

Payload Hash

Next Payload: Attributes

Reserved: 0000

Payload Length: 20

Data: 80AEFC5EA1F421789068A21B520A1E7700000008

Payload Attributes

Next Payload: None

Reserved: 0000

Payload Length: 8

type: ISAKMP_CFG_ACK

Reserved: 00

Identifier: 0000

Sev=Info/4 IKE/0x43000013 11/05/2001 14:02:43.829 83

SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 161.44.127.196

Sev=Decode/11 IKE/0x43000001 11/05/2001 14:02:43.831 84

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Transaction

(Flags: (Encryption

MessageID: 19973167

Length: 469762048

Payload Hash

Next Payload: Attributes

Reserved: 0000

Payload Length: 20

Data: 9309A365C01503CB0B89B888D530494500000056

Payload Attributes

Next Payload: None

Reserved: 0000

Payload Length: 86

type: ISAKMP_CFG_REQUEST

Reserved: 00

Identifier: 0000

(IPv4 Address: (empty

(IPv4 Netmask: (empty

(IPv4 DNS: (empty

(IPv4 NBNS (WINS): (empty

(Address Expiry: (empty

Application Version: Cisco Systems VPN Client 3.0.8

(Cisco extension: Banner: (empty

(Cisco extension: Save PWD: (empty

(Cisco extension: Default Domain Name: (empty

(Cisco extension: Split Include: (empty

(Cisco extension: Do PFS: (empty

(Cisco extension: NAT traversal UDP Port: (empty

Sev=Debug/8 IKE/0x4300004B 11/05/2001 14:02:43.832 85

,Starting DPD timer for IKE SA* 081801C8, sa->state = 4
,sa->dpd_peer_enabled = 1, sa->dpd_timer = 081803FC
sa->dpd.worry_freq = 5000

Sev=Info/5 IKE/0x4300002F 11/05/2001 14:02:43.879 86

Received ISAKMP packet: peer = 161.44.127.196

Sev=Decode/11 IKE/0x43000001 11/05/2001 14:02:43.882 87

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Transaction

(Flags: (Encryption

MessageID: 67319719

Length: 236

Payload Hash

Next Payload: Attributes

Reserved: 0000

Payload Length: 20

Data: 8722B4CDB825174DAB03CBC052241CC6000000B7

Payload Attributes

Next Payload: None

Reserved: 0000

Payload Length: 183

type: ISAKMP_CFG_REPLY

Reserved: 00

Identifier: 0000

IPv4 Address: 4.0.0.0

IPv4 DNS: 4.0.0.0

IPv4 DNS: 4.0.0.0

IPv4 NBNS (WINS): 4.0.0.0

IPv4 NBNS (WINS): 4.0.0.0

:Cisco extension: Banner: rtp-vpn-cluster-2-nat
.Cisco Systems Inc

.UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED

Cisco extension: Save PWD: No

Cisco extension: Default Domain Name: cisco.com

Cisco extension: NAT traversal UDP Port: 3221200488

Cisco extension: Do PFS: No

Sev=Info/4 IKE/0x43000014 11/05/2001 14:02:43.882 88

RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from
161.44.127.196

Sev=Info/5 IKE/0x43000010 11/05/2001 14:02:43.883 89

, :MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS
value = 10.82.240.214

Sev=Info/5 IKE/0x43000010 11/05/2001 14:02:43.883 90

, :(MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_DNS(1
value = 64.102.6.247

Sev=Info/5 IKE/0x43000010 11/05/2001 14:02:43.883 91

, :(MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_DNS(2

value = 171.68.226.120

Sev=Info/5 IKE/0x43000010 11/05/2001 14:02:43.883 92

(MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NBNS(1
a.k.a. WINS) : , value = 64.102.2.124)

Sev=Info/5 IKE/0x43000010 11/05/2001 14:02:43.883 93

(MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NBNS(2
a.k.a. WINS): , value = 171.68.235.228)

Sev=Info/5 IKE/0x4300000E 11/05/2001 14:02:43.883 94

,MODE_CFG_REPLY: Attribute = MODECFG_UNITY_BANNER
.value = rtp-vpn-cluster-2-nat: Cisco Systems Inc

.UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED

Sev=Info/5 IKE/0x4300000D 11/05/2001 14:02:43.883 95

, :MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD
value = 0x00000000

Sev=Info/5 IKE/0x4300000E 11/05/2001 14:02:43.883 96

, :MODE_CFG_REPLY: Attribute = MODECFG_UNITY_DEFDOMAIN
value = cisco.com

Sev=Info/5 IKE/0x4300000D 11/05/2001 14:02:43.883 97

,MODE_CFG_REPLY: Attribute = MODECFG_UNITY_UDP_NAT_PORT
value = 0x00002710

Sev=Info/5 IKE/0x4300000D 11/05/2001 14:02:43.883 98

, :MODE_CFG_REPLY: Attribute = MODECFG_UNITY_PFS
value = 0x00000000

Sev=Info/4 CM/0x43100019 11/05/2001 14:02:43.899 99

Mode Config data received

Sev=Info/5 IKE/0x43000055 11/05/2001 14:03:03.938 100

Received a key request from Driver for IP address
GW IP = 161.44.127.196 ,161.44.127.196

Sev=Info/4 IKE/0x43000013 11/05/2001 14:03:03.939 101

(SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID
to 161.44.127.196

Sev=Decode/11 IKE/0x43000001 11/05/2001 14:03:03.942 102

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Quick Mode

(Flags: (Encryption

MessageID: 371035BB

Length: 469762048

Payload Hash

Next Payload: Security Association

Reserved: 0000

Payload Length: 20

Data: C4134662EC838D6032DC22393A14ECA90A0002B8

Payload Security Association

Next Payload: Nonce

Reserved: 0000

Payload Length: 696

DOI: IPsec

(Situation:(SIT_IDENTITY_ONLY

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 1

Protocol-Id: PROTO_IPSEC_ESP

SPI Size: 4

of transfroms: 1 #

SPI: 76AF9EAA

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP_3DES

Reserved2: 0000

Authentication Algorithm: MD5

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 34

Proposal #: 1

Protocol-Id: PROTO_IPCOMP

SPI Size: 2

of transfroms: 1 #

SPI: 11B2

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 24

Transform #: 1

Transform-Id: IPCOMP_LZS

Reserved2: 0000

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 2

Protocol-Id: PROTO_IPSEC_ESP

SPI Size: 4

of transfroms: 1 #

SPI: 76AF9EAA

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP_3DES

Reserved2: 0000

Authentication Algorithm: SHA1

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 34

Proposal #: 2

Protocol-Id: PROTO_IPCOMP

SPI Size: 2

of transfroms: 1 #

SPI: 2AC8

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 24

Transform #: 1

Transform-Id: IPCOMP_LZS

Reserved2: 0000

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 3

Protocol-Id: PROTO_IPSEC_ESP

SPI Size: 4

of transfroms: 1 #

SPI: 76AF9EAA

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP_3DES

Reserved2: 0000

Authentication Algorithm: MD5

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 4

Protocol-Id: PROTO_IPSEC_ESP

SPI Size: 4

of transfroms: 1 #

SPI: 76AF9EAA

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP_3DES

Reserved2: 0000

Authentication Algorithm: SHA1

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 5

Protocol-Id: PROTO_IPSEC_ESP

SPI Size: 4

of transfroms: 1 #

SPI: 76AF9EAA

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP_DES

Reserved2: 0000

Authentication Algorithm: MD5

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 34

Proposal #: 5

Protocol-Id: PROTO_IPCOMP

SPI Size: 2

of transfroms: 1 #

SPI: 2A25

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 24

Transform #: 1

Transform-Id: IPCOMP_LZS

Reserved2: 0000

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 6

Protocol-Id: PROTO_IPSEC_ESP

SPI Size: 4

of transfroms: 1 #

SPI: 76AF9EAA

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP_DES

Reserved2: 0000

Authentication Algorithm: SHA1

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 34

Proposal #: 6

Protocol-Id: PROTO_IPCOMP

SPI Size: 2

of transfroms: 1 #

SPI: B7EB

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 24

Transform #: 1

Transform-Id: IPCOMP_LZS

Reserved2: 0000

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 7

Protocol-Id: PROTO_IPSEC_ESP

SPI Size: 4

of transfroms: 1 #

SPI: 76AF9EAA

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP_DES

Reserved2: 0000

Authentication Algorithm: MD5

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 8

Protocol-Id: PROTO_IPSEC_ESP

SPI Size: 4

of transfroms: 1 #

SPI: 76AF9EAA

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP_DES

Reserved2: 0000

Authentication Algorithm: SHA1

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 9

Protocol-Id: PROTO_IPSEC_ESP

SPI Size: 4

of transfroms: 1 #

SPI: 76AF9EAA

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP_NULL

Reserved2: 0000

Authentication Algorithm: MD5

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 34

Proposal #: 9

Protocol-Id: PROTO_IPCOMP

SPI Size: 2

of transfroms: 1 #

SPI: 9637

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 24

Transform #: 1

Transform-Id: IPCOMP_LZS

Reserved2: 0000

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 10

Protocol-Id: PROTO_IPSEC_ESP

SPI Size: 4

of transfroms: 1 #

SPI: 76AF9EAA

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP_NULL

Reserved2: 0000

Authentication Algorithm: SHA1

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 34

Proposal #: 10

Protocol-Id: PROTO_IPCOMP

SPI Size: 2

of transfroms: 1 #

SPI: 68E9

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 24

Transform #: 1

Transform-Id: IPCOMP_LZS

Reserved2: 0000

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 11

Protocol-Id: PROTO_IPSEC_ESP

SPI Size: 4

of transfroms: 1 #

SPI: 76AF9EAA

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP_NULL

Reserved2: 0000

Authentication Algorithm: MD5

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: None

Reserved: 0000

Payload Length: 40

Proposal #: 12

Protocol-Id: PROTO_IPSEC_ESP

SPI Size: 4

of transfroms: 1 #

SPI: 76AF9EAA

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP_NULL

Reserved2: 0000

Authentication Algorithm: SHA1

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Nonce

Next Payload: Identification

Reserved: 0000

Payload Length: 24

Data: B63EA44802CE0827FDEEEEC71751188416F73CE30500000C

Payload Identification

Next Payload: Identification

Reserved: 0000

Payload Length: 12

ID Type: IPv4 Address

Protocol ID (UDP/TCP, etc...): 0

Port: 0

ID Data: 10.82.240.214

Payload Identification

Next Payload: None

Reserved: 0000

Payload Length: 12

ID Type: IPv4 Address

Protocol ID (UDP/TCP, etc...): 0

Port: 0

ID Data: 161.44.127.196

Sev=Info/5 IKE/0x43000055 11/05/2001 14:03:03.943 103

Received a key request from Driver for IP address
GW IP = 161.44.127.196 ,10.10.10.255

Sev=Info/4 IKE/0x43000013 11/05/2001 14:03:03.944 104

(SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID
to 161.44.127.196

Sev=Decode/11 IKE/0x43000001 11/05/2001 14:03:03.947 105

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Quick Mode

(Flags: (Encryption

MessageID: F94C749C

Length: 469762048

Payload Hash

Next Payload: Security Association

Reserved: 0000

Payload Length: 20

Data: 7FEE58A44DA5DC279D9DE7D1C8651ED80A0002B8

Payload Security Association

Next Payload: Nonce

Reserved: 0000

Payload Length: 696

DOI: IPsec

(Situation:(SIT_IDENTITY_ONLY

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 1

Protocol-Id: PROTO_IPSEC_ESP

SPI Size: 4

of transfroms: 1 #

SPI: 47269429

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP_3DES

Reserved2: 0000

Authentication Algorithm: MD5

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 34

Proposal #: 1

Protocol-Id: PROTO_IPCOMP

SPI Size: 2

of transfroms: 1 #

SPI: 37A9

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 24

Transform #: 1

Transform-Id: IPCOMP_LZS

Reserved2: 0000

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 2

Protocol-Id: PROTO_IPSEC_ESP

SPI Size: 4

of transfroms: 1 #

SPI: 47269429

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP_3DES

Reserved2: 0000

Authentication Algorithm: SHA1

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 34

Proposal #: 2

Protocol-Id: PROTO_IPCOMP

SPI Size: 2

of transfroms: 1 #

SPI: D8C8

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 24

Transform #: 1

Transform-Id: IPCOMP_LZS

Reserved2: 0000

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 3

Protocol-Id: PROTO_IPSEC_ESP

SPI Size: 4

of transfroms: 1 #

SPI: 47269429

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP_3DES

Reserved2: 0000

Authentication Algorithm: MD5

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 4

Protocol-Id: PROTO_IPSEC_ESP

SPI Size: 4

of transfroms: 1 #

SPI: 47269429

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP_3DES

Reserved2: 0000

Authentication Algorithm: SHA1

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 5

Protocol-Id: PROTO_IPSEC_ESP

SPI Size: 4

of transfroms: 1 #

SPI: 47269429

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP_DES

Reserved2: 0000

Authentication Algorithm: MD5

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 34

Proposal #: 5

Protocol-Id: PROTO_IPCOMP

SPI Size: 2

of transfroms: 1 #

SPI: B4AA

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 24

Transform #: 1

Transform-Id: IPCOMP_LZS

Reserved2: 0000

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 6

Protocol-Id: PROTO_IPSEC_ESP

SPI Size: 4

of transfroms: 1 #

SPI: 47269429

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP_DES

Reserved2: 0000

Authentication Algorithm: SHA1

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 34

Proposal #: 6

Protocol-Id: PROTO_IPCOMP

SPI Size: 2

of transfroms: 1 #

SPI: 10D5

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 24

Transform #: 1

Transform-Id: IPCOMP_LZS

Reserved2: 0000

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 7

Protocol-Id: PROTO_IPSEC_ESP

SPI Size: 4

of transfroms: 1 #

SPI: 47269429

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP_DES

Reserved2: 0000

Authentication Algorithm: MD5

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 8

Protocol-Id: PROTO_IPSEC_ESP

SPI Size: 4

of transfroms: 1 #

SPI: 47269429

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP_DES

Reserved2: 0000

Authentication Algorithm: SHA1

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 9

Protocol-Id: PROTO_IPSEC_ESP

SPI Size: 4

of transfroms: 1 #

SPI: 47269429

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP_NULL

Reserved2: 0000

Authentication Algorithm: MD5

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 34

Proposal #: 9

Protocol-Id: PROTO_IPCOMP

SPI Size: 2

of transfroms: 1 #

SPI: 6A1B

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 24

Transform #: 1

Transform-Id: IPCOMP_LZS

Reserved2: 0000

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 10

Protocol-Id: PROTO_IPSEC_ESP

SPI Size: 4

of transfroms: 1 #

SPI: 47269429

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP_NULL

Reserved2: 0000

Authentication Algorithm: SHA1

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 34

Proposal #: 10

Protocol-Id: PROTO_IPCOMP

SPI Size: 2

of transfroms: 1 #

SPI: 784E

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 24

Transform #: 1

Transform-Id: IPCOMP_LZS

Reserved2: 0000

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 11

Protocol-Id: PROTO_IPSEC_ESP

SPI Size: 4

of transfroms: 1 #

SPI: 47269429

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP_NULL

Reserved2: 0000

Authentication Algorithm: MD5

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: None

Reserved: 0000

Payload Length: 40

Proposal #: 12

Protocol-Id: PROTO_IPSEC_ESP

SPI Size: 4

of transfroms: 1 #

SPI: 47269429

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP_NULL

Reserved2: 0000

Authentication Algorithm: SHA1

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Nonce

Next Payload: Identification

Reserved: 0000

Payload Length: 24

Data: DCDE51C03B32B7694D2125080EFD647FADD61DDC0500000C

Payload Identification

Next Payload: Identification

Reserved: 0000

Payload Length: 12

ID Type: IPv4 Address

Protocol ID (UDP/TCP, etc...): 0

Port: 0

ID Data: 10.82.240.214

Payload Identification

Next Payload: None

Reserved: 0000

Payload Length: 16

ID Type: IPv4 Subnet

Protocol ID (UDP/TCP, etc...): 0

Port: 0

ID Data: 0.0.0.0/0.0.0.0

Sev=Debug/8 IKE/0x4300004B 11/05/2001 14:03:03.948 106

,Starting DPD timer for IKE SA* 081801C8, sa->state = 4
,sa->dpd_peer_enabled = 1, sa->dpd_timer = 081803FC
sa->dpd.worry_freq = 5000

Sev=Info/5 IKE/0x4300002F 11/05/2001 14:03:03.948 107

Received ISAKMP packet: peer = 161.44.127.196

Sev=Decode/11 IKE/0x43000001 11/05/2001 14:03:03.951 108

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Transaction

(Flags: (Encryption

MessageID: 67319719

Length: 236

PACKET MAY BE CORRUPT... RESERVED FIELD NOT SET TO ZERO

Sev=Info/4 IKE/0x43000014 11/05/2001 14:03:03.952 109

RECEIVING <<< ISAKMP OAK TRANS *(HASH,) from 161.44.127.196

Sev=Warning/3 IKE/0x83000057 11/05/2001 14:03:03.952 110

Received malformed message or negotiation no longer active
(message id: 0x67319719)

Sev=Info/5 IKE/0x4300002F 11/05/2001 14:03:03.952 111

Received ISAKMP packet: peer = 161.44.127.196

Sev=Decode/11 IKE/0x43000001 11/05/2001 14:03:03.955 112

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Transaction

(Flags: (Encryption

MessageID: 67319719

Length: 236

PACKET MAY BE CORRUPT... RESERVED FIELD NOT SET TO ZERO

Sev=Info/4 IKE/0x43000014 11/05/2001 14:03:03.955 113

RECEIVING <<< ISAKMP OAK TRANS *(HASH,) from 161.44.127.196

Sev=Warning/3 IKE/0x83000057 11/05/2001 14:03:03.955 114

Received malformed message or negotiation no longer active
(message id: 0x67319719)

Sev=Info/4 IPSEC/0x43700014 11/05/2001 14:03:03.955 115

Deleted all keys

Sev=Info/4 IPSEC/0x43700010 11/05/2001 14:03:03.955 116

Created a new key structure

Sev=Info/5 IKE/0x43000055 11/05/2001 14:03:03.955 117

,Received a key request from Driver for IP address 24.93.67.64
GW IP = 161.44.127.196

Sev=Warning/3 IKE/0xC3000002 11/05/2001 14:03:03.955 118

Function initialize_qm failed with an error code of 0x00000000
(INITIATE:805)

Sev=Info/5 IKE/0x4300002F 11/05/2001 14:03:03.990 119

Received ISAKMP packet: peer = 161.44.127.196

Sev=Decode/11 IKE/0x43000001 11/05/2001 14:03:03.993 120

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Informational

(Flags: (Encryption

MessageID: D10A6912

Length: 92

Payload Hash

Next Payload: Notification

Reserved: 0000

Payload Length: 20

Data: 52138C38D364E77DB5980565F7A8C8EF00000028

Payload Notification

Next Payload: None

Reserved: 0000

Payload Length: 40

DOI: IPsec

Protocol-ID: PROTO_ISAKMP

Spi Size: 16

Notify Type: STATUS_RESP_LIFETIME

SPI: DACB1B32139742E7630E88F067C1B0B5

Data: 800B0001000C000400015180

Sev=Info/4 IKE/0x43000014 11/05/2001 14:03:03.994 121

(RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:STATUS_RESP_LIFETIME
from 161.44.127.196

Sev=Info/5 IKE/0x43000044 11/05/2001 14:03:03.994 122

RESPONDER-LIFETIME notify has value of 86400 seconds

Sev=Info/5 IKE/0x43000046 11/05/2001 14:03:03.994 123

This SA has already been alive for 38 seconds, setting expiry to
seconds from now 86362

Sev=Info/5 IKE/0x4300002F 11/05/2001 14:03:03.994 124

Received ISAKMP packet: peer = 161.44.127.196

Sev=Decode/11 IKE/0x43000001 11/05/2001 14:03:03.997 125

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Quick Mode

(Flags: (Encryption

MessageID: BB351037

Length: 172

Payload Hash

Next Payload: Security Association

Reserved: 0000

Payload Length: 20

Data: 3A6CD2078E1F4CF6ACC2810A77A88BF90A000034

Payload Security Association

Next Payload: Nonce

Reserved: 0000

Payload Length: 52

DOI: IPsec

(Situation:(SIT_IDENTITY_ONLY

Payload Proposal

Next Payload: None

Reserved: 0000

Payload Length: 40

Proposal #: 1

Protocol-Id: PROTO_IPSEC_ESP

SPI Size: 4

of transfroms: 1 #

SPI: 0C38AE25

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP_3DES

Reserved2: 0000

Life Type: Seconds

Life Duration (Hex): 0020C49B

Encapsulation Mode: Tunnel

Authentication Algorithm: MD5

Payload Nonce

Next Payload: Identification

Reserved: 0000

Payload Length: 24

Data: 57184AEFF363B10FC00D05A543D6B0B01067274F0500000C

Payload Identification

Next Payload: Identification

Reserved: 0000

Payload Length: 12

ID Type: IPv4 Address

Protocol ID (UDP/TCP, etc...): 0

Port: 0

ID Data: 10.82.240.214

Payload Identification

Next Payload: Notification

Reserved: 0000

Payload Length: 12

ID Type: IPv4 Address

Protocol ID (UDP/TCP, etc...): 0

Port: 0

ID Data: 161.44.127.196

Payload Notification

Next Payload: None

Reserved: 0000

Payload Length: 24

DOI: IPsec

Protocol-ID: PROTO_IPSEC_ESP

Spi Size: 4

Notify Type: STATUS_RESP_LIFETIME

SPI: 0C38AE25

Data: 80010001800270 80

Sev=Info/4 IKE/0x43000014 11/05/2001 14:03:03.997 126

,RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID
NOTIFY:STATUS_RESP_LIFETIME) from 161.44.127.196

Sev=Info/5 IKE/0x43000044 11/05/2001 14:03:03.997 127

RESPONDER-LIFETIME notify has value of 28800 seconds

Sev=Info/4 IKE/0x43000013 11/05/2001 14:03:03.997 128

SENDING >>> ISAKMP OAK QM *(HASH) to 161.44.127.196

Sev=Decode/11 IKE/0x43000001 11/05/2001 14:03:03.1000 129

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Quick Mode

(Flags: (Encryption

MessageID: 371035BB

Length: 469762048

Payload Hash

Next Payload: None

Reserved: 0000

Payload Length: 20

Data: C2456940045DC9C608E0D4D6FA62822400000000

Sev=Info/5 IKE/0x43000058 11/05/2001 14:03:03.1000 130

= Loading IPsec SA (Message ID = 0xBB351037 OUTBOUND SPI
(0x0C38AE25 INBOUND SPI = 0x76AF9EAA

Sev=Info/5 IKE/0x43000025 11/05/2001 14:03:04.001 131

Loaded OUTBOUND ESP SPI: 0x0C38AE25

Sev=Info/5 IKE/0x43000026 11/05/2001 14:03:04.001 132

Loaded INBOUND ESP SPI: 0x76AF9EAA

Sev=Info/4 CM/0x4310001A 11/05/2001 14:03:04.001 133

One secure connection established

Sev=Info/5 IKE/0x4300002F 11/05/2001 14:03:04.007 134

Received ISAKMP packet: peer = 161.44.127.196

Sev=Decode/11 IKE/0x43000001 11/05/2001 14:03:04.010 135

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Quick Mode

(Flags: (Encryption

MessageID: 9C744CF9

Length: 180

Payload Hash

Next Payload: Security Association

Reserved: 0000

Payload Length: 20

Data: 4591C989262C4F863FD2DC911E7DBA900A000034

Payload Security Association

Next Payload: Nonce

Reserved: 0000

Payload Length: 52

DOI: IPsec

(Situation:(SIT_IDENTITY_ONLY

Payload Proposal

Next Payload: None

Reserved: 0000

Payload Length: 40

Proposal #: 1

Protocol-Id: PROTO_IPSEC_ESP

SPI Size: 4

of transfroms: 1 #

SPI: 503F4CC5

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP_3DES

Reserved2: 0000

Life Type: Seconds

Life Duration (Hex): 0020C49B

Encapsulation Mode: Tunnel

Authentication Algorithm: MD5

Payload Nonce

Next Payload: Identification

Reserved: 0000

Payload Length: 24

Data: 4DD4873137DD4765208FFCE6087D30A48FA9634F0500000C

Payload Identification

Next Payload: Identification

Reserved: 0000

Payload Length: 12

ID Type: IPv4 Address

Protocol ID (UDP/TCP, etc...): 0

Port: 0

ID Data: 10.82.240.214

Payload Identification

Next Payload: Notification

Reserved: 0000

Payload Length: 16

ID Type: IPv4 Subnet

Protocol ID (UDP/TCP, etc...): 0

Port: 0

ID Data: 0.0.0.0/0.0.0.0

Payload Notification

Next Payload: None

Reserved: 0000

Payload Length: 24

DOI: IPsec

Protocol-ID: PROTO_IPSEC_ESP

Spi Size: 4

Notify Type: STATUS_RESP_LIFETIME

SPI: 503F4CC5

Data: 8001000180027080

```
Sev=Info/4 IKE/0x43000014 11/05/2001 14:03:04.011 136

,RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID
    NOTIFY:STATUS_RESP_LIFETIME) from 161.44.127.196

Sev=Info/5 IKE/0x43000044 11/05/2001 14:03:04.011 137

 RESPONDER-LIFETIME notify has value of 28800 seconds

Sev=Info/4 IKE/0x43000013 11/05/2001 14:03:04.011 138

  SENDING >>> ISAKMP OAK QM *(HASH) to 161.44.127.196

Sev=Decode/11 IKE/0x43000001 11/05/2001 14:03:04.014 139

                                                ISAKMP Header

                                Initiator COOKIE: DACB1B32139742E7

                                Responder COOKIE: 630E88F067C1B0B5

                                        Next Payload: Hash

                                                Ver: 10

                                    Exchange Type: Quick Mode

                                           (Flags: (Encryption

                                          MessageID: F94C749C

                                            Length: 469762048

                                                 Payload Hash

                                        Next Payload: None

                                            Reserved: 0000

                                        Payload Length: 20

                                Data: 8AF3A2608A24AB1FB8C8ECA82B2CC99200000000

Sev=Info/5 IKE/0x43000058 11/05/2001 14:03:04.014 140

= Loading IPsec SA (Message ID = 0x9C744CF9 OUTBOUND SPI
                    (0x503F4CC5 INBOUND SPI = 0x47269429

Sev=Info/5 IKE/0x43000025 11/05/2001 14:03:04.015 141

                    Loaded OUTBOUND ESP SPI: 0x503F4CC5

Sev=Info/5 IKE/0x43000026 11/05/2001 14:03:04.015 142

                    Loaded INBOUND ESP SPI: 0x47269429

 Sev=Info/4 CM/0x43100022 11/05/2001 14:03:04.015 143

                    .Additional Phase 2 SA established

 Sev=Info/4 IPSEC/0x43700010 11/05/2001 14:03:05.018 144

                                Created a new key structure
```

```
Sev=Info/4 IPSEC/0x4370000F 11/05/2001 14:03:05.018 145
            Added key with SPI=0x25ae380c into key list
Sev=Info/4 IPSEC/0x43700010 11/05/2001 14:03:05.018 146
                           Created a new key structure
Sev=Info/4 IPSEC/0x4370000F 11/05/2001 14:03:05.018 147
            Added key with SPI=0xaa9eaf76 into key list
Sev=Info/4 IPSEC/0x4370000F 11/05/2001 14:03:05.018 148
            Added key with SPI=0xc54c3f50 into key list
Sev=Info/4 IPSEC/0x43700010 11/05/2001 14:03:05.019 149
                           Created a new key structure
Sev=Info/4 IPSEC/0x4370000F 11/05/2001 14:03:05.019 150
            Added key with SPI=0x29942647 into key list
  Sev=Info/6 IKE/0x4300003D 11/05/2001 14:03:55.528 151
Sending DPD request to 161.44.127.196, seq# = 1153554501
  Sev=Info/4 IKE/0x43000013 11/05/2001 14:03:55.529 152
(SENDING >>> ISAKMP OAK INFO *(HASH, NOTIFY:DPD_REQUEST
                                        to 161.44.127.196
Sev=Decode/11 IKE/0x43000001 11/05/2001 14:03:55.531 153
                                        ISAKMP Header
                        Initiator COOKIE: DACB1B32139742E7
                        Responder COOKIE: 630E88F067C1B0B5
                                    Next Payload: Hash
                                            Ver: 10
                                Exchange Type: Informational
                                    (Flags: (Encryption
                                    MessageID: 791ED04C
                                      Length: 469762048
                                           Payload Hash
                                  Next Payload: Notification
                                        Reserved: 0000
                                    Payload Length: 20
                    Data: C0E66CDA100E9C77C75A46AD3AECA51C00000020
```

Payload Notification

Next Payload: None

Reserved: 0000

Payload Length: 32

DOI: IPsec

Protocol-ID: PROTO_ISAKMP

Spi Size: 16

Notify Type: DPD_R_U_THERE

SPI: DACB1B32139742E7630E88F067C1B0B5

Data: 44C1D845

Sev=Info/4 IKE/0x43000013 11/05/2001 14:03:55.532 154

(SENDING >>> ISAKMP OAK INFO *(HASH, NOTIFY:HEARTBEAT
to 161.44.127.196

Sev=Decode/11 IKE/0x43000001 11/05/2001 14:03:55.535 155

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Informational

(Flags: (Encryption

MessageID: 68218ECF

Length: 469762048

Payload Hash

Next Payload: Notification

Reserved: 0000

Payload Length: 20

Data: E705E1CE2854A92CA7DEC4C04AB6654B0000001C

Payload Notification

Next Payload: None

Reserved: 0000

Payload Length: 28

DOI: IPsec

Protocol-ID: PROTO_ISAKMP

Spi Size: 16

Notify Type: STATUS_ALTIGA_KEEPALIVE

SPI: DACB1B32139742E7630E88F067C1B0B5

:Data

Sev=Info/6 IKE/0x43000052 11/05/2001 14:03:55.535 156

Sent a ping on the IKE SA

Sev=Info/5 IKE/0x4300002F 11/05/2001 14:03:55.575 157

Received ISAKMP packet: peer = 161.44.127.196

Sev=Decode/11 IKE/0x43000001 11/05/2001 14:03:55.578 158

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Informational

(Flags: (Encryption

MessageID: E63FE567

Length: 84

Payload Hash

Next Payload: Notification

Reserved: 0000

Payload Length: 20

Data: FD8DA1906266110 87DD2B8DC3DDDE72900000020

Payload Notification

Next Payload: None

Reserved: 0000

Payload Length: 32

DOI: IPsec

Protocol-ID: PROTO_ISAKMP

```
                                                    Spi Size: 16

                                          Notify Type: DPD_R_U_THERE_ACK

                                  SPI: DACB1B32139742E7630E88F067C1B0B5

                                                    Data: 44C1D845


          Sev=Info/4 IKE/0x43000014 11/05/2001 14:03:55.579 159

          (RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:DPD_ACK
                                               from 161.44.127.196

          Sev=Info/5 IKE/0x4300003F 11/05/2001 14:03:55.579 160

          = Received DPD ACK from 161.44.127.196, seq# received
                        seq# expected = 1153554501 ,1153554501
```

مركز VPN 3000

```
SEV=8 IKEDBG/0 RPT=199 172.18.124.241 14:18:18.630 11/05/2001 1
                     : RECEIVED Message (msgid=0) with payloads
      (HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + VENDOR (13
                                          VENDOR (13) + VENDOR +
                          NONE (0) ... total length : 562 + (13)

SEV=9 IKEDBG/0 RPT=200 172.18.124.241 14:18:18.630 11/05/2001 4

                                          processing SA payload

SEV=9 IKEDBG/0 RPT=201 172.18.124.241 14:18:18.630 11/05/2001 5

                                          processing ke payload

SEV=9 IKEDBG/0 RPT=202 172.18.124.241 14:18:18.630 11/05/2001 6

                                              processing ISA_KE

 SEV=9 IKEDBG/1 RPT=59 172.18.124.241 14:18:18.630 11/05/2001 7

                                        processing nonce payload

 SEV=9 IKEDBG/1 RPT=60 172.18.124.241 14:18:18.630 11/05/2001 8

                                                    Processing ID

SEV=9 IKEDBG/47 RPT=38 172.18.124.241 14:18:18.630 11/05/2001 9

                                        processing VID payload

SEV=9 IKEDBG/49 RPT=37 172.18.124.241 14:18:18.630 11/05/2001 10

                                         Received xauth V6 VID

SEV=9 IKEDBG/47 RPT=39 172.18.124.241 14:18:18.630 11/05/2001 11

                                        processing VID payload

SEV=9 IKEDBG/49 RPT=38 172.18.124.241 14:18:18.630 11/05/2001 12
```

```
                                                    Received DPD VID

SEV=9 IKEDBG/47 RPT=40 172.18.124.241 14:18:18.630 11/05/2001 13

                                                processing VID payload

SEV=9 IKEDBG/49 RPT=39 172.18.124.241 14:18:18.630 11/05/2001 14

                                        Received Cisco Unity client VID

SEV=9 IKEDBG/23 RPT=12 172.18.124.241 14:18:18.630 11/05/2001 15

                           Starting group lookup for peer 172.18.124.241

                         SEV=8 AUTHDBG/1 RPT=4 14:18:18.630 11/05/2001 16
                                                AUTH_Open() returns 3

                           SEV=7 AUTH/12 RPT=4 14:18:18.630 11/05/2001 17
                                Authentication session opened: handle = 3

                         SEV=8 AUTHDBG/3 RPT=6 14:18:18.630 11/05/2001 18
                                                (AUTH_PutAttrTable(3, 61ea34

                         SEV=8 AUTHDBG/6 RPT=3 14:18:18.630 11/05/2001 19
                               (AUTH_GroupAuthenticate(3, 51a88f0, 431480

                        SEV=8 AUTHDBG/59 RPT=6 14:18:18.630 11/05/2001 20
                                                (AUTH_BindServer(511a7bc, 0, 0

                        SEV=9 AUTHDBG/69 RPT=6 14:18:18.630 11/05/2001 21
                        ,Auth Server e3199c has been bound to ACB 511a7bc
                                                            sessions = 1

                        SEV=8 AUTHDBG/65 RPT=6 14:18:18.630 11/05/2001 22
                                                (AUTH_CreateTimer(511a7bc, 0, 0

                        SEV=9 AUTHDBG/72 RPT=6 14:18:18.630 11/05/2001 23
                                             Reply timer created: handle = 340017

                        SEV=8 AUTHDBG/61 RPT=6 14:18:18.630 11/05/2001 24
                                                (AUTH_BuildMsg(511a7bc, 0, 0

                        SEV=8 AUTHDBG/64 RPT=6 14:18:18.630 11/05/2001 25
                                                (AUTH_StartTimer(511a7bc, 0, 0

                         SEV=9 AUTHDBG/73 RPT=6 14:18:18.630 11/05/2001 26
             ,Reply timer started: handle = 340017, timestamp = 97010941
                                                            timeout = 30000

                        SEV=8 AUTHDBG/62 RPT=6 14:18:18.630 11/05/2001 27
                                                (AUTH_SndRequest(511a7bc, 0, 0

                       SEV=8 AUTHDBG/50 RPT=11 14:18:18.630 11/05/2001 28
                                                (IntDB_Decode(37f34d0, 115

                       SEV=8 AUTHDBG/47 RPT=11 14:18:18.630 11/05/2001 29
                                                    (IntDB_Xmt(511a7bc

                        SEV=9 AUTHDBG/71 RPT=6 14:18:18.630 11/05/2001 30
                                                        xmit_cnt = 1

                       SEV=8 AUTHDBG/47 RPT=12 14:18:18.630 11/05/2001 31
                                                    (IntDB_Xmt(511a7bc
```

```
                    SEV=8 AUTHDBG/49 RPT=6 14:18:18.730 11/05/2001 32
                                    (IntDB_Match(511a7bc, 2f1a854

                    SEV=8 AUTHDBG/63 RPT=6 14:18:18.730 11/05/2001 33
                                    (AUTH_RcvReply(511a7bc, 0, 0

                   SEV=8 AUTHDBG/50 RPT=12 14:18:18.730 11/05/2001 34
                                     (IntDB_Decode(2f1a854, 104

                    SEV=8 AUTHDBG/48 RPT=6 14:18:18.730 11/05/2001 35
                                            (IntDB_Rcv(511a7bc

                    SEV=8 AUTHDBG/66 RPT=6 14:18:18.730 11/05/2001 36
                                    (AUTH_DeleteTimer(511a7bc, 0, 0

                    SEV=9 AUTHDBG/74 RPT=6 14:18:18.730 11/05/2001 37
          Reply timer stopped: handle = 340017, timestamp = 97010951

                    SEV=8 AUTHDBG/58 RPT=6 14:18:18.730 11/05/2001 38
                                    (AUTH_Callback(511a7bc, 0, 0

       SEV=6 AUTH/39 RPT=5 172.18.124.241 14:18:18.730 11/05/2001 39
           ,Authentication successful: handle = 3, server = Internal
                                                  group = ipsecgroup

    SEV=7 IKEDBG/0 RPT=203 172.18.124.241 14:18:18.730 11/05/2001 40
                                                  [Group [ipsecgroup
                                    (Found Phase 1 Group (ipsecgroup

                    SEV=8 AUTHDBG/4 RPT=4 14:18:18.730 11/05/2001 41
                                    (AUTH_GetAttrTable(3, 61ea7c

     SEV=7 IKEDBG/14 RPT=4 172.18.124.241 14:18:18.730 11/05/2001 42
                                                  [Group [ipsecgroup
                                Authentication configured for Internal

                    SEV=8 AUTHDBG/2 RPT=4 14:18:18.730 11/05/2001 43
                                                      (AUTH_Close(3

    SEV=9 IKEDBG/0 RPT=204 172.18.124.241 14:18:18.730 11/05/2001 44
                                                  [Group [ipsecgroup
                                                   processing IKE SA

    SEV=8 IKEDBG/0 RPT=205 172.18.124.241 14:18:18.730 11/05/2001 45
                                                  [Group [ipsecgroup
                    Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
                                        :Parsing received transform
                    :Phase 1 failure against global IKE proposal # 1
                           :Mismatched attr types for class Hash Alg
                                                    Rcv'd: SHA
                                                    Cfg'd: MD5

    SEV=8 IKEDBG/0 RPT=206 172.18.124.241 14:18:18.730 11/05/2001 50
                                                  [Group [ipsecgroup
                    :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=207 172.18.124.241 14:18:18.730 11/05/2001 53
                                                  [Group [ipsecgroup
                    :Phase 1 failure against global IKE proposal # 3
                           :Mismatched attr types for class Hash Alg
```

```
                                                                Rcv'd: SHA
                                                                Cfg'd: MD5

          SEV=8 IKEDBG/0 RPT=208 172.18.124.241 14:18:18.730 11/05/2001 56
                                                        [Group [ipsecgroup
                        :Phase 1 failure against global IKE proposal # 4
                               :Mismatched attr types for class DH Group
                                                    Rcv'd: Oakley Group 2
                                                    Cfg'd: Oakley Group 1

          SEV=8 IKEDBG/0 RPT=209 172.18.124.241 14:18:18.730 11/05/2001 60
                                                        [Group [ipsecgroup
                        :Phase 1 failure against global IKE proposal # 5
                               :Mismatched attr types for class DH Group
                                                    Rcv'd: Oakley Group 2
                                                    Cfg'd: Oakley Group 1

          SEV=8 IKEDBG/0 RPT=210 172.18.124.241 14:18:18.730 11/05/2001 64
                                                        [Group [ipsecgroup
                        :Phase 1 failure against global IKE proposal # 6
                               :Mismatched attr types for class DH Group
                                                    Rcv'd: Oakley Group 2
                                                    Cfg'd: Oakley Group 7

           SEV=7 IKEDBG/28 RPT=4 172.18.124.241 14:18:18.730 11/05/2001 68
                                                        [Group [ipsecgroup
                             IKE SA Proposal # 1, Transform # 2 acceptable
                                                 Matches global IKE entry # 1

                        SEV=8 AUTHDBG/60 RPT=6 14:18:18.730 11/05/2001 70
                                          (AUTH_UnbindServer(511a7bc, 0, 0

                        SEV=9 AUTHDBG/70 RPT=6 14:18:18.730 11/05/2001 71
Auth Server e3199c has been unbound from ACB 511a7bc, sessions = 0

                        SEV=8 AUTHDBG/10 RPT=4 14:18:18.730 11/05/2001 72
                                           (AUTH_Int_FreeAuthCB(511a7bc

                        SEV=9 AUTHDBG/19 RPT=4 14:18:18.730 11/05/2001 73
                                          instance = 4, clone_instance = 0

                           SEV=7 AUTH/13 RPT=4 14:18:18.730 11/05/2001 74
                                Authentication session closed: handle = 3

           SEV=9 IKEDBG/0 RPT=211 172.18.124.241 14:18:18.760 11/05/2001 75
                                                        [Group [ipsecgroup
                                        constructing ISA_SA for isakmp

          SEV=9 IKEDBG/0 RPT=212 172.18.124.241 14:18:18.760 11/05/2001 76
                                                        [Group [ipsecgroup
                                                  constructing ke payload

           SEV=9 IKEDBG/1 RPT=61 172.18.124.241 14:18:18.760 11/05/2001 77
                                                        [Group [ipsecgroup
                                                constructing nonce payload

               SEV=9 IKE/0 RPT=5 172.18.124.241 14:18:18.760 11/05/2001 78
                                                        [Group [ipsecgroup
                                             ...Generating keys for Responder

           SEV=9 IKEDBG/1 RPT=62 172.18.124.241 14:18:18.760 11/05/2001 79
                                                        [Group [ipsecgroup
                                                           constructing ID
```

```
                SEV=9 IKEDBG/0 RPT=213 14:18:18.760 11/05/2001 80
                                                [Group [ipsecgroup
                                            construct hash payload

SEV=9 IKEDBG/0 RPT=214 172.18.124.241 14:18:18.760 11/05/2001 81
                                                [Group [ipsecgroup
                                                computing hash

SEV=9 IKEDBG/46 RPT=12 172.18.124.241 14:18:18.760 11/05/2001 82
                                                [Group [ipsecgroup
                                  constructing Cisco Unity VID payload

SEV=9 IKEDBG/46 RPT=13 172.18.124.241 14:18:18.760 11/05/2001 83
                                                [Group [ipsecgroup
                                     constructing xauth V6 VID payload

SEV=9 IKEDBG/46 RPT=14 172.18.124.241 14:18:18.760 11/05/2001 84
                                                [Group [ipsecgroup
                                          constructing dpd vid payload

SEV=9 IKEDBG/46 RPT=15 172.18.124.241 14:18:18.760 11/05/2001 85
                                                [Group [ipsecgroup
                                            constructing VID payload

 SEV=9 IKEDBG/48 RPT=5 172.18.124.241 14:18:18.760 11/05/2001 86
                                                [Group [ipsecgroup
                                                Send Altiga GW VID

SEV=8 IKEDBG/0 RPT=215 172.18.124.241 14:18:18.760 11/05/2001 87
                            : SENDING Message (msgid=0) with payloads
                                  HDR + SA (1) ... total length : 344

SEV=8 IKEDBG/0 RPT=216 172.18.124.241 14:18:18.790 11/05/2001 88
                           : RECEIVED Message (msgid=0) with payloads
   HDR + HASH (8) + NOTIFY (11) + NONE (0) ... total length : 76

SEV=9 IKEDBG/0 RPT=217 172.18.124.241 14:18:18.790 11/05/2001 90
                                                [Group [ipsecgroup
                                                   processing hash

SEV=9 IKEDBG/0 RPT=218 172.18.124.241 14:18:18.790 11/05/2001 91
                                                [Group [ipsecgroup
                                                computing hash

SEV=9 IKEDBG/0 RPT=219 172.18.124.241 14:18:18.790 11/05/2001 92
                                                [Group [ipsecgroup
                                          Processing Notify payload

SEV=9 IKEDBG/0 RPT=220 172.18.124.241 14:18:18.790 11/05/2001 93
                                                [Group [ipsecgroup
                                            constructing blank hash

SEV=9 IKEDBG/0 RPT=221 172.18.124.241 14:18:18.790 11/05/2001 94
                                                [Group [ipsecgroup
                                             constructing qm hash

SEV=8 IKEDBG/0 RPT=222 172.18.124.241 14:18:18.790 11/05/2001 95
                             : SENDING Message (msgid=6ea8e2bc) with payloads
                                      HDR + HASH (8) ... total length : 100

SEV=8 IKEDBG/0 RPT=223 172.18.124.241 14:18:23.290 11/05/2001 97
                            : RECEIVED Message (msgid=6ea8e2bc) with payloads
     HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 85
```

```
  SEV=9 IKEDBG/1 RPT=63 14:18:23.290 11/05/2001 99
                              !process_attr(): Enter

 SEV=9 IKEDBG/1 RPT=64 14:18:23.290 11/05/2001 100
                   .Processing cfg reply attributes

 SEV=8 AUTHDBG/1 RPT=5 14:18:23.290 11/05/2001 101
                               AUTH_Open() returns 4

   SEV=7 AUTH/12 RPT=5 14:18:23.290 11/05/2001 102
         Authentication session opened: handle = 4

 SEV=8 AUTHDBG/3 RPT=7 14:18:23.290 11/05/2001 103
                        (AUTH_PutAttrTable(4, 61ea34

 SEV=8 AUTHDBG/5 RPT=2 14:18:23.290 11/05/2001 104
              (AUTH_Authenticate(4, 2f1b480, 460ec0

SEV=8 AUTHDBG/59 RPT=7 14:18:23.290 11/05/2001 105
                     (AUTH_BindServer(511760c, 0, 0

SEV=9 AUTHDBG/69 RPT=7 14:18:23.290 11/05/2001 106
 ,Auth Server e3199c has been bound to ACB 511760c
                                       sessions = 1

SEV=8 AUTHDBG/65 RPT=7 14:18:23.290 11/05/2001 107
                    (AUTH_CreateTimer(511760c, 0, 0

SEV=9 AUTHDBG/72 RPT=7 14:18:23.290 11/05/2001 108
               Reply timer created: handle = 360014

SEV=8 AUTHDBG/61 RPT=7 14:18:23.290 11/05/2001 109
                       (AUTH_BuildMsg(511760c, 0, 0

SEV=8 AUTHDBG/64 RPT=7 14:18:23.290 11/05/2001 110
                     (AUTH_StartTimer(511760c, 0, 0

SEV=9 AUTHDBG/73 RPT=7 14:18:23.290 11/05/2001 111
 = Reply timer started: handle = 360014, timestamp
                          timeout = 30000 ,97011407

SEV=8 AUTHDBG/62 RPT=7 14:18:23.290 11/05/2001 112
                     (AUTH_SndRequest(511760c, 0, 0

SEV=8 AUTHDBG/50 RPT=13 14:18:23.290 11/05/2001 113
                          (IntDB_Decode(37f34d0, 102

SEV=8 AUTHDBG/47 RPT=13 14:18:23.290 11/05/2001 114
                                  (IntDB_Xmt(511760c

 SEV=9 AUTHDBG/71 RPT=7 14:18:23.290 11/05/2001 115
                                       xmit_cnt = 1

SEV=8 AUTHDBG/47 RPT=14 14:18:23.290 11/05/2001 116
                                  (IntDB_Xmt(511760c

 SEV=8 AUTHDBG/49 RPT=7 14:18:23.390 11/05/2001 117
                       (IntDB_Match(511760c, 2f1bb8c

 SEV=8 AUTHDBG/63 RPT=7 14:18:23.390 11/05/2001 118
                       (AUTH_RcvReply(511760c, 0, 0

SEV=8 AUTHDBG/50 RPT=14 14:18:23.390 11/05/2001 119
                          (IntDB_Decode(2f1bb8c, 116
```

```
                                SEV=8 AUTHDBG/48 RPT=7 14:18:23.390 11/05/2001 120
                                                        (IntDB_Rcv(511760c

                                SEV=8 AUTHDBG/66 RPT=7 14:18:23.390 11/05/2001 121
                                                (AUTH_DeleteTimer(511760c, 0, 0

                                SEV=9 AUTHDBG/74 RPT=7 14:18:23.390 11/05/2001 122
                           Reply timer stopped: handle = 360014, timestamp = 97011417

                                SEV=8 AUTHDBG/58 RPT=7 14:18:23.390 11/05/2001 123
                                                    (AUTH_Callback(511760c, 0, 0

                        SEV=6 AUTH/4 RPT=2 172.18.124.241 14:18:23.390 11/05/2001 124
                                        = Authentication successful: handle = 4, server
                                                      Internal, user = ipsecuser

                                 SEV=8 AUTHDBG/3 RPT=8 14:18:23.390 11/05/2001 125
                                                    (AUTH_PutAttrTable(4, f0d688

                                SEV=8 AUTHDBG/60 RPT=7 14:18:23.390 11/05/2001 126
                                                (AUTH_UnbindServer(511760c, 0, 0

                                SEV=9 AUTHDBG/70 RPT=7 14:18:23.390 11/05/2001 127
                           ,Auth Server e3199c has been unbound from ACB 511760c
                                                                sessions = 0

                                SEV=8 AUTHDBG/59 RPT=8 14:18:23.390 11/05/2001 128
                                                    (AUTH_BindServer(511760c, 0, 0

                                SEV=9 AUTHDBG/69 RPT=8 14:18:23.390 11/05/2001 129
                                 ,Auth Server e3199c has been bound to ACB 511760c
                                                                sessions = 1

                                SEV=8 AUTHDBG/65 RPT=8 14:18:23.390 11/05/2001 130
                                                (AUTH_CreateTimer(511760c, 0, 0

                                SEV=9 AUTHDBG/72 RPT=8 14:18:23.390 11/05/2001 131
                                            Reply timer created: handle = 370014

                                SEV=8 AUTHDBG/61 RPT=8 14:18:23.390 11/05/2001 132
                                                    (AUTH_BuildMsg(511760c, 0, 0

                                SEV=8 AUTHDBG/64 RPT=8 14:18:23.390 11/05/2001 133
                                                    (AUTH_StartTimer(511760c, 0, 0

                                SEV=9 AUTHDBG/73 RPT=8 14:18:23.390 11/05/2001 134
                                 = Reply timer started: handle = 370014, timestamp
                                                      timeout = 30000 ,97011417

                                SEV=8 AUTHDBG/62 RPT=8 14:18:23.390 11/05/2001 135
                                                    (AUTH_SndRequest(511760c, 0, 0

                               SEV=8 AUTHDBG/50 RPT=15 14:18:23.390 11/05/2001 136
                                                      (IntDB_Decode(1f9d5b8, 44

                               SEV=8 AUTHDBG/47 RPT=15 14:18:23.390 11/05/2001 137
                                                        (IntDB_Xmt(511760c

                                SEV=9 AUTHDBG/71 RPT=8 14:18:23.390 11/05/2001 138
                                                            xmit_cnt = 1

                               SEV=8 AUTHDBG/47 RPT=16 14:18:23.390 11/05/2001 139
                                                        (IntDB_Xmt(511760c
```

```
SEV=8 AUTHDBG/49 RPT=8 14:18:23.490 11/05/2001 140
                    (IntDB_Match(511760c, 2f1af60

SEV=8 AUTHDBG/63 RPT=8 14:18:23.490 11/05/2001 141
                     (AUTH_RcvReply(511760c, 0, 0

SEV=8 AUTHDBG/50 RPT=16 14:18:23.490 11/05/2001 142
                      (IntDB_Decode(2f1af60, 104

SEV=8 AUTHDBG/48 RPT=8 14:18:23.490 11/05/2001 143
                                (IntDB_Rcv(511760c

SEV=8 AUTHDBG/66 RPT=8 14:18:23.490 11/05/2001 144
                   (AUTH_DeleteTimer(511760c, 0, 0

SEV=9 AUTHDBG/74 RPT=8 14:18:23.490 11/05/2001 145
 = Reply timer stopped: handle = 370014, timestamp
                                          97011427

SEV=8 AUTHDBG/58 RPT=8 14:18:23.490 11/05/2001 146
                     (AUTH_Callback(511760c, 0, 0

   SEV=6 AUTH/39 RPT=6 14:18:23.490 11/05/2001 147
                                       172.18.124.241
   = Authentication successful: handle = 4, server
                     Internal, group = ipsecgroup

 SEV=8 AUTHDBG/3 RPT=9 14:18:23.490 11/05/2001 148
                     (AUTH_PutAttrTable(4, f0d688

SEV=8 AUTHDBG/60 RPT=8 14:18:23.490 11/05/2001 149
                   (AUTH_UnbindServer(511760c, 0, 0

   SEV=9 AUTHDBG/70 RPT=8 14:18:23.490 11/05/2001 150
,Auth Server e3199c has been unbound from ACB 511760c
                                        sessions = 0

SEV=8 AUTHDBG/59 RPT=9 14:18:23.490 11/05/2001 151
                     (AUTH_BindServer(511760c, 0, 0

SEV=9 AUTHDBG/69 RPT=9 14:18:23.490 11/05/2001 152
 ,Auth Server e3199c has been bound to ACB 511760c
                                        sessions = 1

SEV=8 AUTHDBG/65 RPT=9 14:18:23.490 11/05/2001 153
                   (AUTH_CreateTimer(511760c, 0, 0

SEV=9 AUTHDBG/72 RPT=9 14:18:23.490 11/05/2001 154
               Reply timer created: handle = 380014

SEV=8 AUTHDBG/61 RPT=9 14:18:23.490 11/05/2001 155
                     (AUTH_BuildMsg(511760c, 0, 0

SEV=8 AUTHDBG/64 RPT=9 14:18:23.490 11/05/2001 156
                     (AUTH_StartTimer(511760c, 0, 0

SEV=9 AUTHDBG/73 RPT=9 14:18:23.490 11/05/2001 157
 = Reply timer started: handle = 380014, timestamp
                       timeout = 30000 ,97011427

SEV=8 AUTHDBG/62 RPT=9 14:18:23.490 11/05/2001 158
                     (AUTH_SndRequest(511760c, 0, 0
```

```
SEV=8 AUTHDBG/50 RPT=17 14:18:23.490 11/05/2001 159
                          (IntDB_Decode(1fe8cc0, 44

SEV=8 AUTHDBG/47 RPT=17 14:18:23.490 11/05/2001 160
                                  (IntDB_Xmt(511760c

 SEV=9 AUTHDBG/71 RPT=9 14:18:23.490 11/05/2001 161
                                       xmit_cnt = 1

SEV=8 AUTHDBG/47 RPT=18 14:18:23.490 11/05/2001 162
                                  (IntDB_Xmt(511760c

 SEV=8 AUTHDBG/49 RPT=9 14:18:23.590 11/05/2001 163
                     (IntDB_Match(511760c, 2f1a99c

 SEV=8 AUTHDBG/63 RPT=9 14:18:23.590 11/05/2001 164
                      (AUTH_RcvReply(511760c, 0, 0

SEV=8 AUTHDBG/50 RPT=18 14:18:23.590 11/05/2001 165
                        (IntDB_Decode(2f1a99c, 104

 SEV=8 AUTHDBG/48 RPT=9 14:18:23.590 11/05/2001 166
                                  (IntDB_Rcv(511760c

 SEV=8 AUTHDBG/66 RPT=9 14:18:23.590 11/05/2001 167
                   (AUTH_DeleteTimer(511760c, 0, 0

 SEV=9 AUTHDBG/74 RPT=9 14:18:23.590 11/05/2001 168
  = Reply timer stopped: handle = 380014, timestamp
                                           97011437

 SEV=8 AUTHDBG/58 RPT=9 14:18:23.590 11/05/2001 169
                      (AUTH_Callback(511760c, 0, 0

    SEV=6 AUTH/39 RPT=7 14:18:23.590 11/05/2001 170
                                       172.18.124.241
    = Authentication successful: handle = 4, server
                      Internal, group = ipsecgroup

  SEV=8 AUTHDBG/4 RPT=5 14:18:23.590 11/05/2001 171
                      (AUTH_GetAttrTable(4, 61ea7c

  SEV=7 IKEDBG/14 RPT=5 14:18:23.590 11/05/2001 172
                                       172.18.124.241
               [Group [ipsecgroup] User [ipsecuser
            Authentication configured for Internal

  SEV=8 AUTHDBG/2 RPT=5 14:18:23.590 11/05/2001 173
                                        (AUTH_Close(4

     SEV=4 IKE/52 RPT=2 14:18:23.590 11/05/2001 174
                                       172.18.124.241
               [Group [ipsecgroup] User [ipsecuser
                   .User (ipsecuser) authenticated

 SEV=9 IKEDBG/0 RPT=224 14:18:23.590 11/05/2001 175
                                       172.18.124.241
               [Group [ipsecgroup] User [ipsecuser
                           constructing blank hash

 SEV=9 IKEDBG/0 RPT=225 14:18:23.590 11/05/2001 176
                                       172.18.124.241
               [Group [ipsecgroup] User [ipsecuser
                           constructing qm hash
```

```
SEV=8 IKEDBG/0 RPT=226 14:18:23.590 11/05/2001 177
                                                172.18.124.241
  : SENDING Message (msgid=938074b7) with payloads
                HDR + HASH (8) ... total length : 60

SEV=8 AUTHDBG/60 RPT=9 14:18:23.590 11/05/2001 179
                    (AUTH_UnbindServer(511760c, 0, 0

SEV=9 AUTHDBG/70 RPT=9 14:18:23.590 11/05/2001 180
,Auth Server e3199c has been unbound from ACB 511760c
                                          sessions = 0

SEV=8 AUTHDBG/10 RPT=5 14:18:23.590 11/05/2001 181
                          (AUTH_Int_FreeAuthCB(511760c

SEV=9 AUTHDBG/19 RPT=5 14:18:23.590 11/05/2001 182
                    instance = 5, clone_instance = 0

   SEV=7 AUTH/13 RPT=5 14:18:23.590 11/05/2001 183
         Authentication session closed: handle = 4

SEV=8 IKEDBG/0 RPT=227 14:18:23.600 11/05/2001 184
                                                172.18.124.241
  : RECEIVED Message (msgid=938074b7) with payloads
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 56

   SEV=9 IKEDBG/1 RPT=65 14:18:23.600 11/05/2001 186
                                !process_attr(): Enter

   SEV=9 IKEDBG/1 RPT=66 14:18:23.600 11/05/2001 187
                          Processing cfg ACK attributes

   SEV=8 IKEDBG/0 RPT=228 14:18:23.600 11/05/2001 188
                                                172.18.124.241
  : RECEIVED Message (msgid=c06b6315) with payloads
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 138

   SEV=9 IKEDBG/1 RPT=67 14:18:23.600 11/05/2001 190
                                !process_attr(): Enter

   SEV=9 IKEDBG/1 RPT=68 14:18:23.600 11/05/2001 191
                       Processing cfg Request attributes

   SEV=9 IKEDBG/1 RPT=69 14:18:23.600 11/05/2001 192
                         !Received IPV4 address request

   SEV=9 IKEDBG/1 RPT=70 14:18:23.600 11/05/2001 193
                        !Received IPV4 net mask request

   SEV=9 IKEDBG/1 RPT=71 14:18:23.600 11/05/2001 194
                    !Received DNS server address request

   SEV=9 IKEDBG/1 RPT=72 14:18:23.600 11/05/2001 195
                  !Received WINS server address request

     SEV=6 IKE/130 RPT=3 14:18:23.600 11/05/2001 196
                                                172.18.124.241
                     [Group [ipsecgroup] User [ipsecuser
Received unsupported transaction mode attribute: 5

     SEV=6 IKE/130 RPT=4 14:18:23.600 11/05/2001 198
                                                172.18.124.241
                     [Group [ipsecgroup] User [ipsecuser
```

```
                                Received unsupported transaction mode attribute: 7

                                SEV=9 IKEDBG/1 RPT=73 14:18:23.600 11/05/2001 200
                                                !Received Banner request

                                SEV=9 IKEDBG/1 RPT=74 14:18:23.600 11/05/2001 201
                                                !Received Save PW request

                                SEV=9 IKEDBG/1 RPT=75 14:18:23.600 11/05/2001 202
                                                !Received Default Domain request

                                SEV=9 IKEDBG/1 RPT=76 14:18:23.600 11/05/2001 203
                                                !Received Split Tunnel Include request

                                SEV=9 IKEDBG/1 RPT=77 14:18:23.600 11/05/2001 204
                                                !Received PFS request

                                SEV=9 IKEDBG/1 RPT=78 14:18:23.600 11/05/2001 205
                                                !Received UDP Port request

                                SEV=9 IKEDBG/31 RPT=2 14:18:23.600 11/05/2001 206
                                                172.18.124.241
                                        [Group [ipsecgroup] User [ipsecuser
                                Obtained IP addr (192.168.10.10) prior to initiating
                                                (Mode Cfg (XAuth enabled

                                SEV=9 IKEDBG/0 RPT=229 14:18:23.600 11/05/2001 208
                                                172.18.124.241
                                        [Group [ipsecgroup] User [ipsecuser
                                                constructing blank hash

                                SEV=9 IKEDBG/0 RPT=230 14:18:23.600 11/05/2001 209
                                                172.18.124.241
                        ..... C0A80A0A F0010000 F0070000 00010004 :0000

                                SEV=9 IKEDBG/0 RPT=231 14:18:23.600 11/05/2001 210
                                                172.18.124.241
                                        [Group [ipsecgroup] User [ipsecuser
                                                constructing qm hash

                                SEV=8 IKEDBG/0 RPT=232 14:18:23.600 11/05/2001 211
                                                172.18.124.241
                                  : SENDING Message (msgid=c06b6315) with payloads
                                        HDR + HASH (8) ... total length : 72

                                SEV=9 IKEDBG/21 RPT=2 14:18:23.640 11/05/2001 213
                                                172.18.124.241
                                        [Group [ipsecgroup] User [ipsecuser
                                  Delay Quick Mode processing, Cert/Trans Exch/RM
                                                DSID in progress

                                  SEV=4 AUTH/21 RPT=33 14:18:23.640 11/05/2001 215
                                                User ipsecuser connected

                                SEV=7 IKEDBG/22 RPT=2 14:18:23.640 11/05/2001 216
                                                172.18.124.241
                                        [Group [ipsecgroup] User [ipsecuser
                                  Resume Quick Mode processing, Cert/Trans Exch/RM
                                                DSID completed

                                    SEV=4 IKE/119 RPT=2 14:18:23.640 11/05/2001 218
                                                172.18.124.241
                                        [Group [ipsecgroup] User [ipsecuser
                                                PHASE 1 COMPLETED
```

```
   SEV=6 IKE/121 RPT=2 14:18:23.640 11/05/2001 219
                                        172.18.124.241
          Keep-alive type for this connection: DPD

SEV=7 IKEDBG/0 RPT=233 14:18:23.640 11/05/2001 220
                                        172.18.124.241
               [Group [ipsecgroup] User [ipsecuser
       (Starting phase 1 rekey timer: 73440000 (ms

SEV=9 IKEDBG/0 RPT=234 14:18:23.640 11/05/2001 221
                                        172.18.124.241
               [Group [ipsecgroup] User [ipsecuser
                            sending notify message

SEV=9 IKEDBG/0 RPT=235 14:18:23.640 11/05/2001 222
                                        172.18.124.241
               [Group [ipsecgroup] User [ipsecuser
                         constructing blank hash

SEV=9 IKEDBG/0 RPT=236 14:18:23.640 11/05/2001 223
                                        172.18.124.241
               [Group [ipsecgroup] User [ipsecuser
                           constructing qm hash

SEV=8 IKEDBG/0 RPT=237 14:18:23.640 11/05/2001 224
                                        172.18.124.241
  : SENDING Message (msgid=2899decd) with payloads
              HDR + HASH (8) ... total length : 88

SEV=8 IKEDBG/0 RPT=238 14:18:23.640 11/05/2001 226
                                        172.18.124.241
 : RECEIVED Message (msgid=7551d208) with payloads
   + (HDR + HASH (8) + SA (1) + NONCE (10) + ID (5
                 ID (5) + NONE (0) ... total leng
                                              th : 792

SEV=9 IKEDBG/0 RPT=239 14:18:23.640 11/05/2001 229
                                        172.18.124.241
               [Group [ipsecgroup] User [ipsecuser
                                 processing hash

SEV=9 IKEDBG/0 RPT=240 14:18:23.640 11/05/2001 230
                                        172.18.124.241
               [Group [ipsecgroup] User [ipsecuser
                            processing SA payload

 SEV=9 IKEDBG/1 RPT=79 14:18:23.640 11/05/2001 231
                                        172.18.124.241
               [Group [ipsecgroup] User [ipsecuser
                         processing nonce payload

 SEV=9 IKEDBG/1 RPT=80 14:18:23.640 11/05/2001 232
                                        172.18.124.241
               [Group [ipsecgroup] User [ipsecuser
                                  Processing ID

    SEV=5 IKE/25 RPT=3 14:18:23.640 11/05/2001 233
                                        172.18.124.241
               [Group [ipsecgroup] User [ipsecuser
   :Received remote Proxy Host data in ID Payload
        Address 192.168.10.10, Protocol 0, Port 0

 SEV=9 IKEDBG/1 RPT=81 14:18:23.640 11/05/2001 236
```

```
                                                    172.18.124.241
                                  [Group [ipsecgroup] User [ipsecuser
                                                     Processing ID

                                      SEV=5 IKE/24 RPT=2 14:18:23.640 11/05/2001 237
                                                    172.18.124.241
                                  [Group [ipsecgroup] User [ipsecuser
                                   :Received local Proxy Host data in ID Payload
                                      Address 172.18.124.132, Protocol 0, Port 0

                                    SEV=8 IKEDBG/0 RPT=241 14:18:23.640 11/05/2001 240
                                            QM IsRekeyed old sa not found by addr

                                      SEV=5 IKE/66 RPT=3 14:18:23.640 11/05/2001 241
                                                    172.18.124.241
                                  [Group [ipsecgroup] User [ipsecuser
                                 IKE Remote Peer configured for SA: ESP-3DES-MD5

                                    SEV=9 IKEDBG/0 RPT=242 14:18:23.640 11/05/2001 243
                                                    172.18.124.241
                                  [Group [ipsecgroup] User [ipsecuser
                                                 processing IPSEC SA

                                    SEV=8 IKEDBG/0 RPT=243 14:18:23.650 11/05/2001 244
                            Proposal # 2, Transform # 1, Type ESP, Id Triple-DES
                                                 :Parsing received transform
                                                       :Phase 2 failure
                                 :Mismatched attr types for class HMAC Algorithm
                                                           Rcv'd: SHA
                                                           Cfg'd: MD5

                                   SEV=7 IKEDBG/27 RPT=3 14:18:23.650 11/05/2001 248
                                                    172.18.124.241
                                  [Group [ipsecgroup] User [ipsecuser
                                 IPSec SA Proposal # 3, Transform # 1 acceptable

                                    SEV=7 IKEDBG/0 RPT=244 14:18:23.650 11/05/2001 250
                                                    172.18.124.241
                                  [Group [ipsecgroup] User [ipsecuser
                                                 !IKE: requesting SPI

                                  SEV=9 IPSECDBG/6 RPT=11 14:18:23.650 11/05/2001 251
                              ,IPSEC key message parse - msgtype 6, len 192, vers 1
                                                 pid 00000000, seq 3, err 0
                        ,type 2, mode 0, state 32, label 0, pad 0, spi 00000000 ,
                                                    encrKeyLen 0, hashKeyL
                           en 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1
                                                 lifetime2 0, dsI ,7762996
                                                                 d 300

                                  SEV=9 IPSECDBG/1 RPT=38 14:18:23.650 11/05/2001 255
                                                 !Processing KEY_GETSPI msg

                                  SEV=7 IPSECDBG/13 RPT=3 14:18:23.650 11/05/2001 256
                                                    Reserved SPI 1910411637

                                    SEV=8 IKEDBG/6 RPT=3 14:18:23.650 11/05/2001 257
                                       IKE got SPI from key engine: SPI = 0x71de9175

                                    SEV=9 IKEDBG/0 RPT=245 14:18:23.650 11/05/2001 258
                                                    172.18.124.241
                                  [Group [ipsecgroup] User [ipsecuser
                                                oakley constucting quick mode
```

```
                                SEV=9 IKEDBG/0 RPT=246 14:18:23.650 11/05/2001 259
                                                                    172.18.124.241
                                                [Group [ipsecgroup] User [ipsecuser
                                                            constructing blank hash

                                SEV=9 IKEDBG/0 RPT=247 14:18:23.650 11/05/2001 260
                                                                    172.18.124.241
                                                [Group [ipsecgroup] User [ipsecuser
                                                      constructing ISA_SA for ipsec

                                   SEV=5 IKE/75 RPT=3 14:18:23.650 11/05/2001 261
                                                                    172.18.124.241
                                                [Group [ipsecgroup] User [ipsecuser
                              Overriding Initiator's IPSec rekeying duration from
                                                          to 28800 seconds 2147483

                                 SEV=9 IKEDBG/1 RPT=82 14:18:23.650 11/05/2001 263
                                                                    172.18.124.241
                                                [Group [ipsecgroup] User [ipsecuser
                                                   constructing ipsec nonce payload

                                 SEV=9 IKEDBG/1 RPT=83 14:18:23.650 11/05/2001 264
                                                                    172.18.124.241
                                                [Group [ipsecgroup] User [ipsecuser
                                                            constructing proxy ID

                                SEV=7 IKEDBG/0 RPT=248 14:18:23.650 11/05/2001 265
                                                                    172.18.124.241
                                                [Group [ipsecgroup] User [ipsecuser
                                                         :Transmitting Proxy Id
                                      Remote host: 192.168.10.10 Protocol 0 Port 0
                                      Local host: 172.18.124.132 Protocol 0 Port 0

                                SEV=7 IKEDBG/0 RPT=249 14:18:23.650 11/05/2001 269
                                                                    172.18.124.241
                                                [Group [ipsecgroup] User [ipsecuser
                             Sending RESPONDER LIFETIME notification to Initiator

                                 SEV=9 IKEDBG/0 RPT=250 14:18:23.650 11/05/2001 271
                                                                    172.18.124.241
                                                [Group [ipsecgroup] User [ipsecuser
                                                         constructing qm hash

SEV=8 IKEDBG/0 RPT=251 172.18.124.241 14:18:23.650 11/05/2001 272
                          : SENDING Message (msgid=7551d208) with payloads
                                      HDR + HASH (8) ... total length : 172

SEV=8 IKEDBG/0 RPT=252 172.18.124.241 14:18:23.650 11/05/2001 274
                          : RECEIVED Message (msgid=6c034bb1) with payloads
                  + (HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5
                                                         NONE (0) ... total leng
                                                                      th : 796

                                SEV=9 IKEDBG/0 RPT=253 14:18:23.650 11/05/2001 277
                                                                    172.18.124.241
                                                [Group [ipsecgroup] User [ipsecuser
                                                        processing hash

                                SEV=9 IKEDBG/0 RPT=254 14:18:23.650 11/05/2001 278
                                                                    172.18.124.241
                                                [Group [ipsecgroup] User [ipsecuser
                                                         processing SA payload

                                 SEV=9 IKEDBG/1 RPT=84 14:18:23.650 11/05/2001 279
```

```
                                                    172.18.124.241
                                    [Group [ipsecgroup] User [ipsecuser
                                              processing nonce payload

                                  SEV=9 IKEDBG/1 RPT=85 14:18:23.650 11/05/2001 280
                                                    172.18.124.241
                                    [Group [ipsecgroup] User [ipsecuser
                                                   Processing ID

                                     SEV=5 IKE/25 RPT=4 14:18:23.650 11/05/2001 281
                                                    172.18.124.241
                                              [Group [ipsecgroup] User [ipsecuser
                                  :Received remote Proxy Host data in ID Payload
                                       Address 192.168.10.10, Protocol 0, Port 0

                                  SEV=9 IKEDBG/1 RPT=86 14:18:23.650 11/05/2001 284
                                                    172.18.124.241
                                    [Group [ipsecgroup] User [ipsecuser
                                                   Processing ID

                                     SEV=5 IKE/34 RPT=2 14:18:23.650 11/05/2001 285
                                                    172.18.124.241
                                              [Group [ipsecgroup] User [ipsecuser
                                 :Received local IP Proxy Subnet data in ID Payload
                                  Address 0.0.0.0, Mask 0.0.0.0, Protocol 0, Port 0

                                 SEV=8 IKEDBG/0 RPT=255 14:18:23.650 11/05/2001 288
                                             QM IsRekeyed old sa not found by addr

                                     SEV=5 IKE/66 RPT=4 14:18:23.650 11/05/2001 289
                                                    172.18.124.241
                                              [Group [ipsecgroup] User [ipsecuser
                                    IKE Remote Peer configured for SA: ESP-3DES-MD5


SEV=9 IKEDBG/0 RPT=256 172.18.124.241 14:18:23.650 11/05/2001 291
                                    [Group [ipsecgroup] User [ipsecuser
                                                 processing IPSEC SA

                                   SEV=8 IKEDBG/0 RPT=257 14:18:23.660 11/05/2001 292
                          Proposal # 2, Transform # 1, Type ESP, Id Triple-DES
                                                :Parsing received transform
                                                       :Phase 2 failure
                                    :Mismatched attr types for class HMAC Algorithm
                                                           Rcv'd: SHA
                                                           Cfg'd: MD5

                                  SEV=7 IKEDBG/27 RPT=4 14:18:23.660 11/05/2001 296
                                                    172.18.124.241
                                              [Group [ipsecgroup] User [ipsecuser
                                    IPSec SA Proposal # 3, Transform # 1 acceptable

                                  SEV=7 IKEDBG/0 RPT=258 14:18:23.660 11/05/2001 298
                                                    172.18.124.241
                                              [Group [ipsecgroup] User [ipsecuser
                                                    !IKE: requesting SPI

                                   SEV=9 IPSECDBG/6 RPT=12 14:18:23.660 11/05/2001 299
                                 ,IPSEC key message parse - msgtype 6, len 192, vers 1
                                 ,pid 00000000, seq 4, 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 7764576
                                                  lifetime2 0, dsId 300
```

```
                SEV=9 IPSECDBG/1 RPT=39 14:18:23.660 11/05/2001 303
                                    !Processing KEY_GETSPI msg

                SEV=7 IPSECDBG/13 RPT=4 14:18:23.660 11/05/2001 304
                                    Reserved SPI 1940396912

                   SEV=8 IKEDBG/6 RPT=4 14:18:23.660 11/05/2001 305
                      IKE got SPI from key engine: SPI = 0x73a81b70

SEV=9 IKEDBG/0 RPT=259 172.18.124.241 14:18:23.660 11/05/2001 306
                                    [Group [ipsecgroup] User [ipsecuser
                                         oakley constucting quick mode

SEV=9 IKEDBG/0 RPT=260 172.18.124.241 14:18:23.660 11/05/2001 307
                                    [Group [ipsecgroup] User [ipsecuser
                                               constructing blank hash

SEV=9 IKEDBG/0 RPT=261 172.18.124.241 14:18:23.660 11/05/2001 308
                                    [Group [ipsecgroup] User [ipsecuser
                                         constructing ISA_SA for ipsec

    SEV=5 IKE/75 RPT=4 172.18.124.241 14:18:23.660 11/05/2001 309
                                    [Group [ipsecgroup] User [ipsecuser
                Overriding Initiator's IPSec rekeying duration from
                                          to 28800 seconds 2147483

 SEV=9 IKEDBG/1 RPT=87 172.18.124.241 14:18:23.660 11/05/2001 311
                                    [Group [ipsecgroup] User [ipsecuser
                                       constructing ipsec nonce payload

 SEV=9 IKEDBG/1 RPT=88 172.18.124.241 14:18:23.660 11/05/2001 312
                                    [Group [ipsecgroup] User [ipsecuser
                                                  constructing proxy ID

SEV=7 IKEDBG/0 RPT=262 172.18.124.241 14:18:23.660 11/05/2001 313
                                    [Group [ipsecgroup] User [ipsecuser
                                                 :Transmitting Proxy Id
                        Remote host: 192.168.10.10 Protocol 0 Port 0
                Local subnet: 0.0.0.0 mask 0.0.0.0 Protocol 0 Port 0

SEV=7 IKEDBG/0 RPT=263 172.18.124.241 14:18:23.660 11/05/2001 317
                                    [Group [ipsecgroup] User [ipsecuser
                Sending RESPONDER LIFETIME notification to Initiator

SEV=9 IKEDBG/0 RPT=264 172.18.124.241 14:18:23.660 11/05/2001 319
                                    [Group [ipsecgroup] User [ipsecuser
                                                  constructing qm hash

SEV=8 IKEDBG/0 RPT=265 172.18.124.241 14:18:23.660 11/05/2001 320
                    : SENDING Message (msgid=6c034bb1) with payloads
                               HDR + HASH (8) ... total length : 176

SEV=8 IKEDBG/0 RPT=266 172.18.124.241 14:18:23.660 11/05/2001 322
                   : RECEIVED Message (msgid=7551d208) with payloads
                     HDR + HASH (8) + NONE (0) ... total length : 48

SEV=9 IKEDBG/0 RPT=267 172.18.124.241 14:18:23.660 11/05/2001 324
                                    [Group [ipsecgroup] User [ipsecuser
                                                    processing hash

SEV=9 IKEDBG/0 RPT=268 172.18.124.241 14:18:23.660 11/05/2001 325
                                    [Group [ipsecgroup] User [ipsecuser
                                                  loading all IPSEC SAs
```

```
SEV=9 IKEDBG/1 RPT=89 172.18.124.241 14:18:23.660 11/05/2001 326
                                [Group [ipsecgroup] User [ipsecuser
                                        !Generating Quick Mode Key

SEV=9 IKEDBG/1 RPT=90 172.18.124.241 14:18:23.660 11/05/2001 327
                                [Group [ipsecgroup] User [ipsecuser
                                        !Generating Quick Mode Key

SEV=7 IKEDBG/0 RPT=269 172.18.124.241 14:18:23.670 11/05/2001 328
                                [Group [ipsecgroup] User [ipsecuser
                                                :Loading host
                                              Dst: 172.18.124.132
                                               Src: 192.168.10.10

   SEV=4 IKE/49 RPT=3 172.18.124.241 14:18:23.670 11/05/2001 330
                                [Group [ipsecgroup] User [ipsecuser
                 (Security negotiation complete for User (ipsecuser
  Responder, Inbound SPI = 0x71de9175, Outbound SPI = 0x2081f1c4

                   SEV=9 IPSECDBG/6 RPT=13 14:18:23.670 11/05/2001 333
                ,IPSEC key message parse - msgtype 1, len 608, vers 1
                ,pid 00000000, seq 0, err 0, type 2, mode 1, state 64
           ,label 0, pad 0, spi 2081f1c4, encrKeyLen 24, hashKeyLen 16
             ,ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 7764576
                                                lifetime2 0, dsId 0

                   SEV=9 IPSECDBG/1 RPT=40 14:18:23.670 11/05/2001 337
                                        !Processing KEY_ADD msg

                   SEV=9 IPSECDBG/1 RPT=41 14:18:23.670 11/05/2001 338
                                    key_msghdr2secassoc(): Enter

                   SEV=7 IPSECDBG/1 RPT=42 14:18:23.670 11/05/2001 339
                                      No USER filter configured

                   SEV=9 IPSECDBG/1 RPT=43 14:18:23.670 11/05/2001 340
                                         KeyProcessAdd: Enter

                   SEV=8 IPSECDBG/1 RPT=44 14:18:23.670 11/05/2001 341
                                  KeyProcessAdd: Adding outbound SA

                   SEV=8 IPSECDBG/1 RPT=45 14:18:23.670 11/05/2001 342
                   KeyProcessAdd: src 172.18.124.132 mask 0.0.0.0, dst
                                      mask 0.0.0.0 192.168.10.10

                   SEV=8 IPSECDBG/1 RPT=46 14:18:23.670 11/05/2001 343
                            KeyProcessAdd: FilterIpsecAddIkeSa success

                   SEV=9 IPSECDBG/6 RPT=14 14:18:23.670 11/05/2001 344
                ,IPSEC key message parse - msgtype 3, len 328, vers 1
                ,pid 00000000, seq 0, err 0, type 2, mode 1, state 32
           ,label 0, pad 0, spi 71de9175, encrKeyLen 24, hashKeyLen 16
             ,ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 7762996
                                                lifetime2 0, dsId 0

                   SEV=9 IPSECDBG/1 RPT=47 14:18:23.670 11/05/2001 348
                                      !Processing KEY_UPDATE msg

                   SEV=9 IPSECDBG/1 RPT=48 14:18:23.670 11/05/2001 349
                                    Update inbound SA addresses

                   SEV=9 IPSECDBG/1 RPT=49 14:18:23.670 11/05/2001 350
                                    key_msghdr2secassoc(): Enter
```

```
                    SEV=7 IPSECDBG/1 RPT=50 14:18:23.670 11/05/2001 351
                                    No USER filter configured

                    SEV=9 IPSECDBG/1 RPT=51 14:18:23.670 11/05/2001 352
                                    KeyProcessUpdate: Enter

                    SEV=8 IPSECDBG/1 RPT=52 14:18:23.670 11/05/2001 353
                                    KeyProcessUpdate: success

                       SEV=8 IKEDBG/7 RPT=3 14:18:23.670 11/05/2001 354
                         IKE got a KEY_ADD msg for SA: SPI = 0x2081f1c4

                     SEV=8 IKEDBG/0 RPT=270 14:18:23.670 11/05/2001 355
                               pitcher: rcv KEY_UPDATE, spi 0x71de9175

   SEV=4 IKE/120 RPT=3 172.18.124.241 14:18:23.670 11/05/2001 356
                                [Group [ipsecgroup] User [ipsecuser
                                 (PHASE 2 COMPLETED (msgid=7551d208

SEV=8 IKEDBG/0 RPT=271 172.18.124.241 14:18:23.690 11/05/2001 357
                : RECEIVED Message (msgid=6c034bb1) with payloads
                  HDR + HASH (8) + NONE (0) ... total length : 48

SEV=9 IKEDBG/0 RPT=272 172.18.124.241 14:18:23.690 11/05/2001 359
                                [Group [ipsecgroup] User [ipsecuser
                                                processing hash

SEV=9 IKEDBG/0 RPT=273 172.18.124.241 14:18:23.690 11/05/2001 360
                                [Group [ipsecgroup] User [ipsecuser
                                             loading all IPSEC SAs

 SEV=9 IKEDBG/1 RPT=91 172.18.124.241 14:18:23.690 11/05/2001 361
                                [Group [ipsecgroup] User [ipsecuser
                                        !Generating Quick Mode Key

 SEV=9 IKEDBG/1 RPT=92 172.18.124.241 14:18:23.690 11/05/2001 362
                                [Group [ipsecgroup] User [ipsecuser
                                        !Generating Quick Mode Key

SEV=7 IKEDBG/0 RPT=274 172.18.124.241 14:18:23.690 11/05/2001 363
                                [Group [ipsecgroup] User [ipsecuser
                                                   :Loading subnet
                                      Dst: 0.0.0.0 mask: 0.0.0.0
                                              Src: 192.168.10.10

    SEV=4 IKE/49 RPT=4 172.18.124.241 14:18:23.690 11/05/2001 365
                                [Group [ipsecgroup] User [ipsecuser
                 (Security negotiation complete for User (ipsecuser
   Responder, Inbound SPI = 0x73a81b70, Outbound SPI = 0xaf8534c2

                    SEV=9 IPSECDBG/6 RPT=15 14:18:23.690 11/05/2001 368
                  ,IPSEC key message parse - msgtype 1, len 608, vers 1
                  ,pid 00000000, seq 0, err 0, type 2, mode 1, state 64
       ,label 0, pad 0, spi af8534c2, encrKeyLen 24, hashKeyLen 16
         ,ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 7764576
                                              lifetime2 0, dsId 0

                    SEV=9 IPSECDBG/1 RPT=53 14:18:23.690 11/05/2001 372
                                    !Processing KEY_ADD msg

                    SEV=9 IPSECDBG/1 RPT=54 14:18:23.690 11/05/2001 373
                                key_msghdr2secassoc(): Enter

                    SEV=7 IPSECDBG/1 RPT=55 14:18:23.690 11/05/2001 374
```

```
                                                    No USER filter configured

                                SEV=9 IPSECDBG/1 RPT=56 14:18:23.690 11/05/2001 375
                                                      KeyProcessAdd: Enter

                                SEV=8 IPSECDBG/1 RPT=57 14:18:23.690 11/05/2001 376
                                           KeyProcessAdd: Adding outbound SA

                                SEV=8 IPSECDBG/1 RPT=58 14:18:23.690 11/05/2001 377
                              KeyProcessAdd: src 0.0.0.0 mask 255.255.255.255, dst
                                                  mask 0.0.0.0 192.168.10.10

                                SEV=8 IPSECDBG/1 RPT=59 14:18:23.690 11/05/2001 378
                                   KeyProcessAdd: FilterIpsecAddIkeSa success

                                SEV=9 IPSECDBG/6 RPT=16 14:18:23.690 11/05/2001 379
                             ,IPSEC key message parse - msgtype 3, len 328, vers 1
                             ,pid 00000000, seq 0, err 0, type 2, mode 1, state 32
                          ,label 0, pad 0, spi 73a81b70, encrKeyLen 24, hashKeyLen 16
                            ,ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 7762996
                                                  lifetime2 0, dsId 0

                                SEV=9 IPSECDBG/1 RPT=60 14:18:23.690 11/05/2001 383
                                                !Processing KEY_UPDATE msg

                                SEV=9 IPSECDBG/1 RPT=61 14:18:23.690 11/05/2001 384
                                               Update inbound SA addresses

                                SEV=9 IPSECDBG/1 RPT=62 14:18:23.690 11/05/2001 385
                                             key_msghdr2secassoc(): Enter

                                SEV=7 IPSECDBG/1 RPT=63 14:18:23.690 11/05/2001 386
                                                    No USER filter configured

                                SEV=9 IPSECDBG/1 RPT=64 14:18:23.690 11/05/2001 387
                                                  KeyProcessUpdate: Enter

                                SEV=8 IPSECDBG/1 RPT=65 14:18:23.690 11/05/2001 388
                                                  KeyProcessUpdate: success

                                  SEV=8 IKEDBG/7 RPT=4 14:18:23.690 11/05/2001 389
                                    IKE got a KEY_ADD msg for SA: SPI = 0xaf8534c2

                                 SEV=8 IKEDBG/0 RPT=275 14:18:23.690 11/05/2001 390
                                          pitcher: rcv KEY_UPDATE, spi 0x73a81b70

SEV=4 IKE/120 RPT=4 172.18.124.241 14:18:23.690 11/05/2001 391
                                  [Group [ipsecgroup] User [ipsecuser
                                    PHASE 2 COMPLETED (msgid=6c034bb1
```

ما الذي يمكن أن يحدث بشكل خاطئ

- تعذر التفاوض مع IPSec أو المضيف لا يستجيب
- يتعذر على المستخدم الاتصال
- لا يوجد تصحيح أخطاء لتركيز VPN 3000 ولا يمكن للمستخدمين الاتصال

تعذر التفاوض مع IPSec أو المضيف لا يستجيب

يوضح تصحيح أخطاء مركز VPN 3000 ما يلي:

```
SEV=4 IKE/22 RPT=5 64.102.55.139 08:59:29.100 02/20/2001 14
No Group found matching badgroup for Pre-shared key peer 64.102.55.139
```

السبب المعتاد لهذه المشكلة هو أن المستخدم يحاول الاتصال باسم مجموعة لم يتم تكوينها.

يتعذر على المستخدم الاتصال

هناك العديد من المشاكل المحتملة إذا لم تتمكن من الاتصال.

- **عامل تصفية مفقود**يوضح تصحيح أخطاء مركز VPN 3000 ما يلي:
```
Filter missing on interface 2, IKE data from Peer x.x.x.x dropped
```
السبب العادي لهذه المشكلة هو أن عامل التصفية مفقود من الواجهة العامة. يجب أن يكون المرشح العام (ولكن يمكن أن يكون المرشح الخاص؛ "none" غير صالح). انتقل إلى **التكوين > الواجهات > Ethernet 2 > تصفية** وجعل عامل التصفية "عام" أو قيمة أخرى (وهذا ليس "بلا").
- **لم يتم تحديد IPSec**رسالة الخطأ هي التالية:
```
.Unable to negotiate IPSec or host did not respond
```

يوضح تصحيح أخطاء مركز VPN 3000 ما يلي:
```
<Terminating connection attempt: IPSEC not permitted for group <group
```
السبب المعتاد لهذه المشكلة هو عدم تحديد IPSec في المجموعة. انتقل إلى **التكوين > إدارة المستخدم > مجموعات ><group>><تعديل> علامة التبويب العامة** وتحقق من تحديد IPSec ضمن بروتوكولات الاتصال النفقي.
- **المستخدم غير موجود في قاعدة البيانات**رسالة الخطأ هي التالية:
```
User Authentication Failed
```
يوضح تصحيح أخطاء مركز VPN 3000 ما يلي:
```
,Authentication rejected: Reason = User was not found handle = 14
<server = Internal, user = <user
```
السبب المعتاد لهذه المشكلة هو أن المستخدم غير موجود في قاعدة بيانات المستخدم. تأكد من إدخال اسم المستخدم الصحيح عند عرض شاشة مصادقة المستخدم.
- **المسار الافتراضي مفقود**يوضح تصحيح أخطاء مركز VPN 3000 ما يلي:
```
Filter missing on interface 0, IKE data from Peer x.x.x.x dropped
```

السبب المعتاد لهذه المشكلة هو أن المسار الافتراضي مفقود. تأكد من وجود مسار افتراضي في التكوين. انتقل إلى **التكوين > النظام > توجيه IP > البوابة الافتراضية** لتحديد البوابة الافتراضية.
- **لا يوجد خيار عنوان IP**رسالة الخطأ هي التالية:
```
.Your IPSec connection has been terminated by the remote peer
```

يوضح تصحيح أخطاء مركز VPN 3000 ما يلي:
```
[ >User [ >user
!IKE rcv'd FAILED IP Addr status
```

السبب المعتاد لهذه المشكلة هو أنه لا يوجد خيار محددا لإعطاء العميل عنوان IP. انتقل إلى **التكوين > النظام > إدارة العنوان > تعيين العنوان** لتحديد خيار.
- **كلمات مرور مختلفة**رسالة الخطأ هي التالية:
```
User authentication failed
```

يوضح تصحيح أخطاء مركز VPN 3000 ما يلي:

```
The calculated HASH doesn't match the received value
```

السبب المعتاد لهذه المشكلة أن المجموعة كلمة على الزبون مختلف من الكلمة يشكل على المركز. تحقق من كلمات المرور على كل من العميل والمركز.

لا يوجد تصحيح أخطاء لتركيز VPN 3000 ولا يمكن للمستخدمين الاتصال

يحتوي المرشح العام للتركيز الافتراضي على قواعد للسماح بحركة المرور التالية:

```
Protocol = UDP, port = 500
Protocol = UDP, port = 10000
Protocol = ESP
Protocol = AH
```

إذا كانت عوامل تصفية مركز VPN 3000 تسمح بحركة المرور هذه، فقد يكون أحد الأجهزة الموجودة بين العميل والمركز حاجزا لبعض هذه المنافذ (ربما أحد جدران الحماية). للتحقق، حاول التوصيل بالمكثف من الشبكة خارج مركز التركيز مباشرة. وإذا نجح ذلك، فهذا يعني أن جهازا بين الكمبيوتر العميل والمركز يعمل على حظر حركة المرور.

معلومات ذات صلة

- صفحة دعم مركز Cisco VPN 3000
- صفحة دعم عميل شبكة VPN من Cisco
- صفحة دعم IPSec
- تنزيل برنامج عميل شبكة VPN
- الدعم التقني والمستندات - Cisco Systems

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