تكوين العديد من عملاء VPN إلى مركز Cisco VPN 3000 باستخدام محاكاة NAT

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين محول ترجمة عنوان الشبكة (NAT-T) بين عملاء Cisco VPN الموجودون خلف ترجمة عنوان المنفذ (PAT)/جهاز nat وموجه Cisco VPN عن بعد. يمكن إستخدام NAT-T بين عملاء شبكة VPN ومجمع VPN، أو بين التركيزات خلف جهاز NAT/PAT. كما يمكن إستخدام NAT-T عند الاتصال بموجه Cisco الذي يشغل برنامج Cisco IOS® وجدار حماية PIX، ومع ذلك، لا تتم مناقشة هذه التكوينات في هذا المستند.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- مركز Cisco من VPN 3000 4.0(1)B
- الوحدات العميلة للشبكات الخاصة الظاهرية (VPN) من Cisco: 3.6.1 و 4.0(3) Rel
- جدار حماية Cisco PIX (جهاز PAT)، الإصدار 6.3(3)

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

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:

هناك عملاء للشبكات الخاصة الظاهرية (VPN) على جهازي الكمبيوتر (10.10.10.2 و 10.10.10.3) خلف جدار حماية PIX. ويتم ببساطة إستخدام PIX في هذا السيناريو كجهاز PAT، ويتم إجراء ضرب على هذه العناوين إلى 171.69.89.78. يمكن إستخدام أي جهاز قادر على ضرب إتصالات داخلية متعددة هنا. يكون العنوان العام لموجه VPN 3000 هو 172.16.172.50. يوضح المثال التالي كيفية تكوين العملاء والمركز بحيث يتم إستخدام NAT-T أثناء تفاوض IKE.

الاصطلاحات

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

معلومات أساسية

بعد اكتمال تفاوض NAT-T، يمكن للبادئ إستخدام أي منفذ (Y) لبروتوكول مخطط بيانات المستخدم العشوائي (UDP). الغاية ميناء ينبغي كنت 4500 UDP، بما أن في 4500 ،Y (UDP)، والمستجيب يستعمل Y ،4500) UDP). يتم إجراء جميع مفاوضات إعادة صياغة مفتاح الإنترنت (IKE) اللاحقة على هذه المنافذ. خلال مفاوضات NAT-T، يفاوض كل من نظراء IPSec منافذ UDP ويقررون أيضا ما إذا كانوا وراء جهاز NAT/PAT. يرسل نظير IPSec خلف جهاز NAT/PAT حزمة IPSec-over-UDP keepalive إلى نظير IPSec الذي ليس خلف جهاز NAT/PAT. يتضمن NAT-T حركة مرور IPSec في مخططات بيانات UDP، باستخدام المنفذ 4500، وبالتالي توفير أجهزة NAT مع معلومات المنفذ. يكتشف NAT-T تلقائيا أي أجهزة NAT، ويغلف حركة مرور IPSec فقط عند الضرورة.

عند تنفيذ IPSec عبر ترجمة NAT على مركز VPN 3000، يأخذ IPSec عبر TCP الأولوية الأولى، ثم NAT-T، وبعد ذلك IPSec على UDP. بشكل افتراضي، NAT-T يكون قيد الإيقاف. أنت تحتاج أن يمكن NAT-T يستعمل خانة إختيار يتواجد في NAT Transparency، تحت ال IPSec تشكيل يتواجد تحت tunneling بروتوكول. أيضا، بالنسبة لأي نفق من شبكة LAN إلى شبكة LAN، يجب تشغيل NAT-T ضمن حقل تكوين شبكة LAN إلى شبكة LAN IPSec NAT-T.

أن يستعمل NAT-T، أنت ينبغي أتمت هذا steps:

1. منفذ مفتوح 4500 على أي جدار حماية قمت بتكوينه أمام مركز الشبكة الخاصة الظاهرية (VPN).
2. أعد تكوين تكوينات IPSec/UDP السابقة باستخدام المنفذ 4500 إلى منفذ مختلف.
3. أختر **Configuration > الواجهات > Ethernet**، واختر الخيار الثاني أو الثالث لمعلمة سياسة التجزئة.تتيح هذه الخيارات حركة المرور عبر أجهزة NAT التي لا تدعم تجزئة IP، ولا تعيق تشغيل أجهزة NAT التي تدعم تجزئة

.IP

تكوين PIX

يتم عرض إخراج التكوين ذي الصلة ل PIX هنا:

جدار حماية PIX

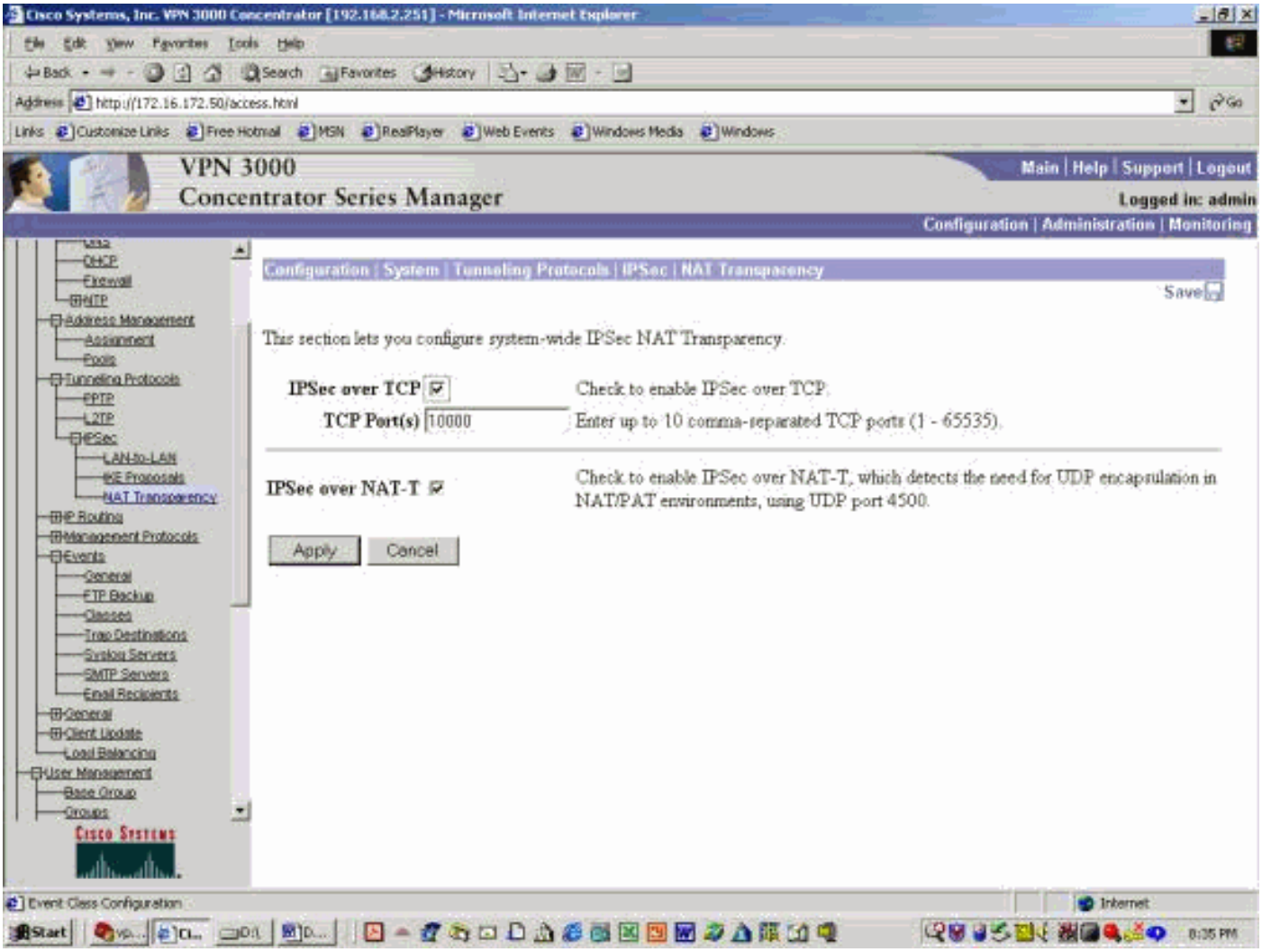
```
#(pix501(config
Saved :
:
(PIX Version 6.3(3
nameif ethernet0 outside security0
nameif ethernet1 inside security100
ip address outside 171.69.89.78 255.255.254.0
ip address inside 10.10.10.1 255.255.255.0
...
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
...
route outside 0.0.0.0 0.0.0.0 171.69.88.1 1
http server enable
http 10.10.10.2 255.255.255.255 inside
...
Cryptochecksum:6990adf6e0e2800ed409ae7364eecc9d
end :

[OK]
```

تكوين مركز VPN 3000

يفترض هذا التكوين العينة أن مركز VPN 3000 قد تم تكوينه بالفعل لاتصال IP، وأنه قد تم إنشاء إتصالات VPN (بخلاف NAT-T) القياسية بالفعل.

لتمكين NAT-T على إصدار مركز VPN 3000 قبل الإصدار 4.1، أختر **تكوينات > نظام > بروتوكولات الاتصال النفقي > IPSec > شفافية NAT**، ثم تحقق من **IPSec عبر** خيار **NAT-T** على المركز كما هو موضح في المثال التالي. ال nat-T يكون خيار إيقاف افتراضيا.

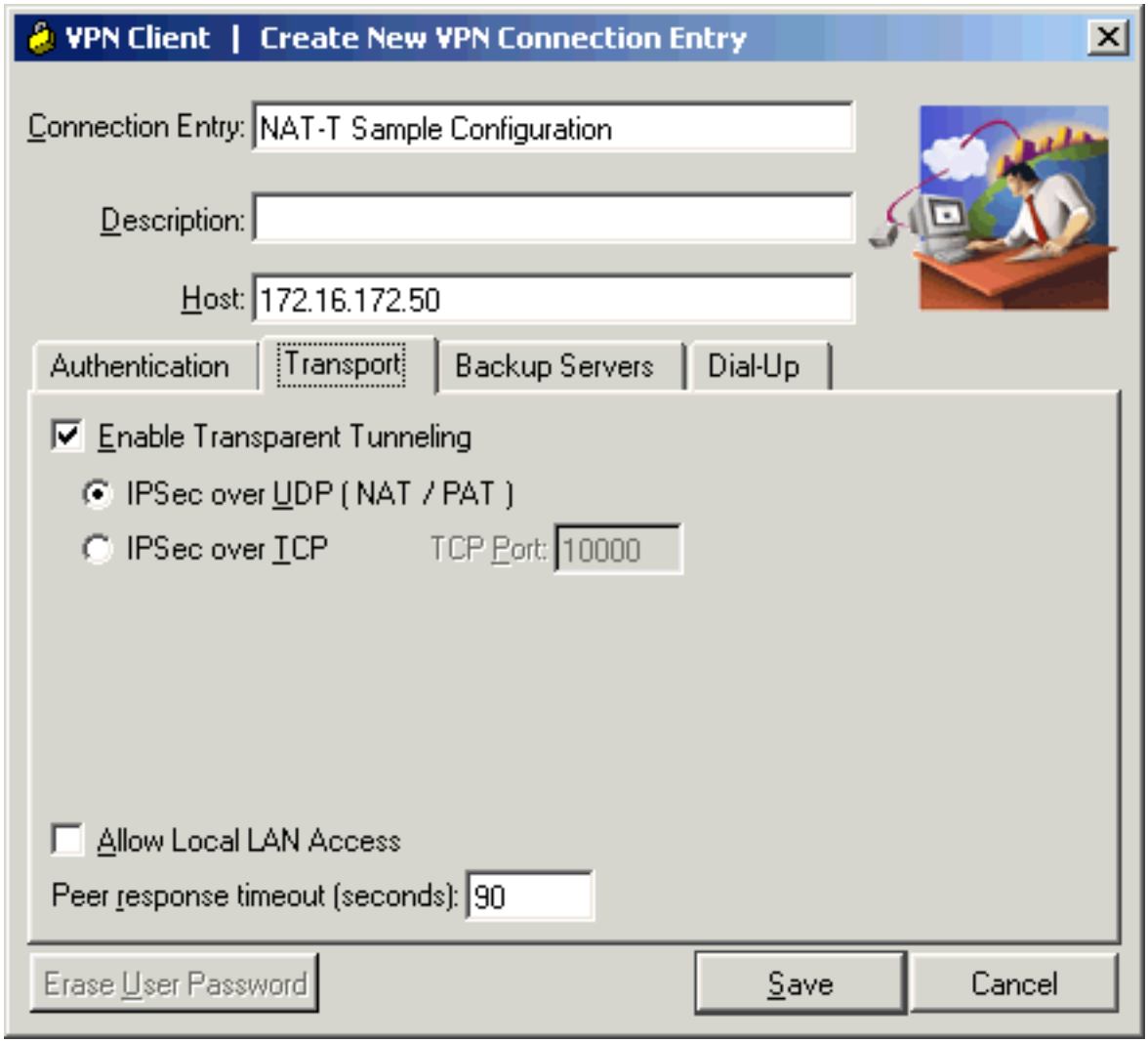
لتمكين NAT-T على مركز VPN الإصدار 4.1 والإصدارات الأحدث، انتقل إلى نفس نافذة شفافية NAT باختيار **التكوين > الاتصال النفقي والأمان > IPSec > شفافية NAT**.



تكوين عميل VPN

لاستخدام NAT-T، تحقق من **تمكين الاتصال النفقي الشفاف**. يوضح المثال التالي هذا الأمر على عميل شبكة VPN أحدث من الإصدار 4.0.

ملاحظة: يتوفر خيار التكوين نفسه على الإصدار x.3 من عميل شبكة VPN.



التحقق من الصحة

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

يتم دعم بعض أوامر **العرض بواسطة** أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر **العرض**.

يمكن العثور على معلومات إضافية حول أستكشاف الأخطاء وإصلاحها في أستكشاف أخطاء أمان IP وإصلاحها - فهم أوامر تصحيح الأخطاء واستخدامها.

التحقق من تكوين PIX

يتم إستخدام هذه الأوامر للتحقق من تكوين PIX:

- **show xlate**—كما هو موضح في الإخراج أدناه، يستخدم PIX منافذ مصدر مختلفة لعملاء VPN، ولكن منافذ الوجهة هي نفسها. يتم تضمين جميع حزم بيانات IPSec باستخدام منفذ UDP 4500. تستخدم مفاوضات إعادة التشكيل اللاحقة أيضا نفس منافذ المصدر والوجهة.

```
pix501(config)# show xlate
                in use, 4 most used 3
(PAT Global 171.69.89.78(1025) Local 10.10.10.3(4500
(PAT Global 171.69.89.78(1026) Local 10.10.10.2(4500
    (PAT Global 171.69.89.78(4) Local 10.10.10.2(500
```

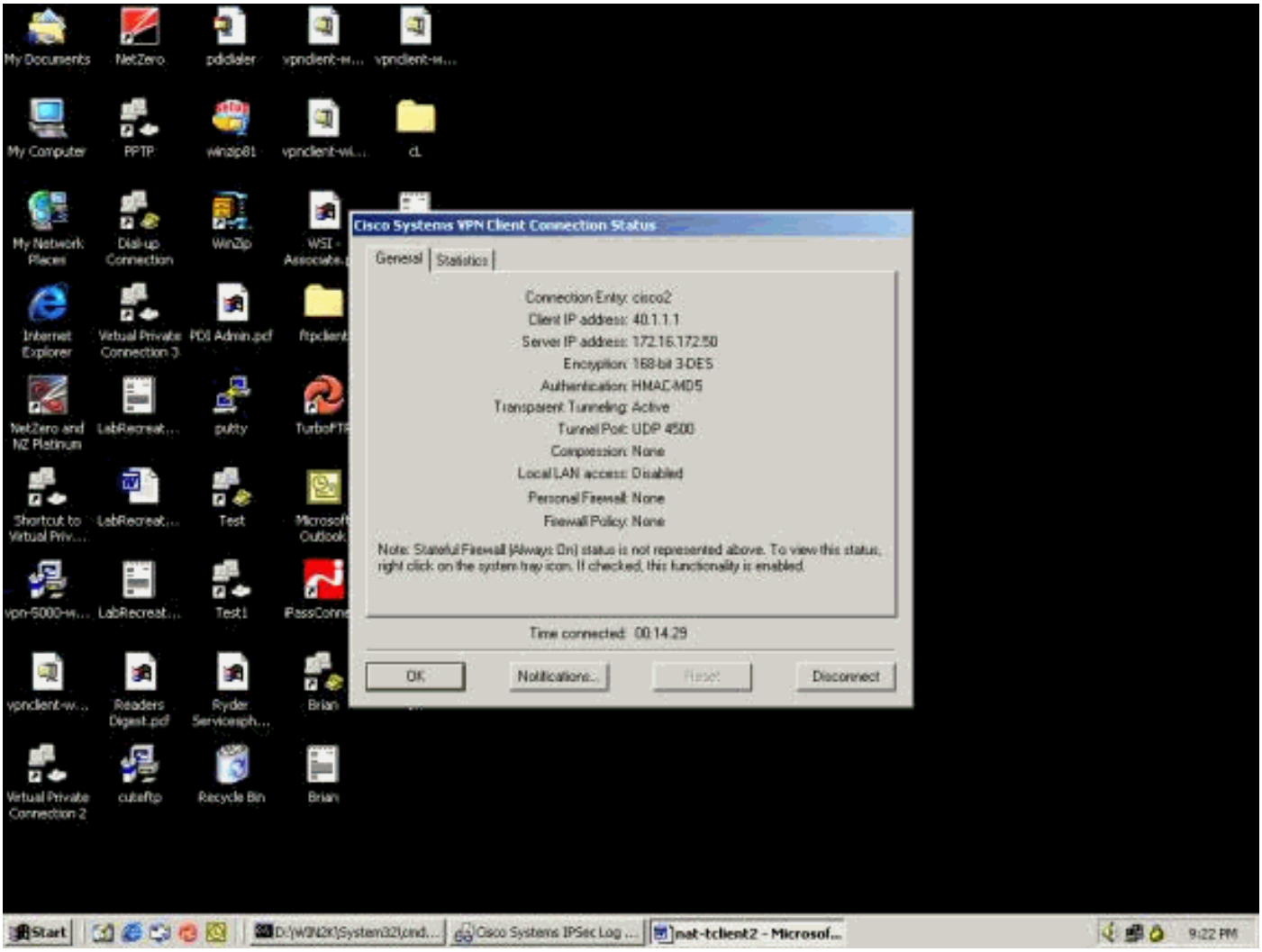
- **show arp**—أستخدم هذا الأمر لعرض جدول بروتوكول تحليل العنوان (ARP) وتحديد ما إذا كانت طلبات ARP

قيد المعالجة أم لا.

```
pix501(config)# show arp
outside 171.69.88.3 00d0.0132.e40a
outside 171.69.88.2 00d0.0133.3c0a
outside 171.69.88.1 0000.0c07.ac7b
  inside 10.10.10.3 0050.dabb.f093
  inside 10.10.10.2 0001.0267.55cc
                          #(pix501(config
```

إحصائيات عميل شبكة VPN

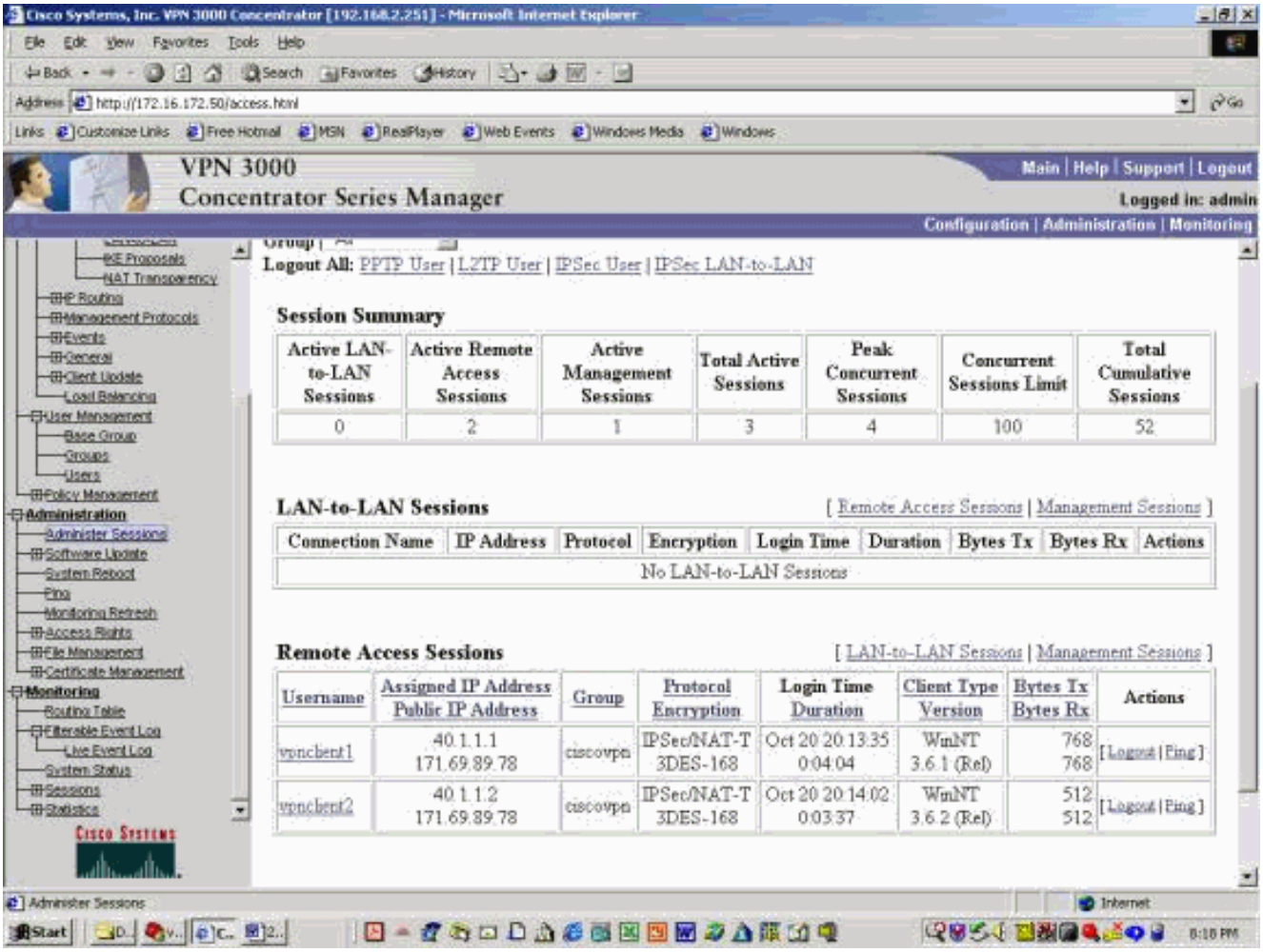
بمجرد إنشاء نفق VPN، انقر بزر الماوس الأيمن على القفل الأصفر واختر **الحالة**. توجد أدناه نافذة مماثلة. لاحظ أن منفذ النفق هو UDP 4500، والذي يثبت أنك تستخدم NAT-T.



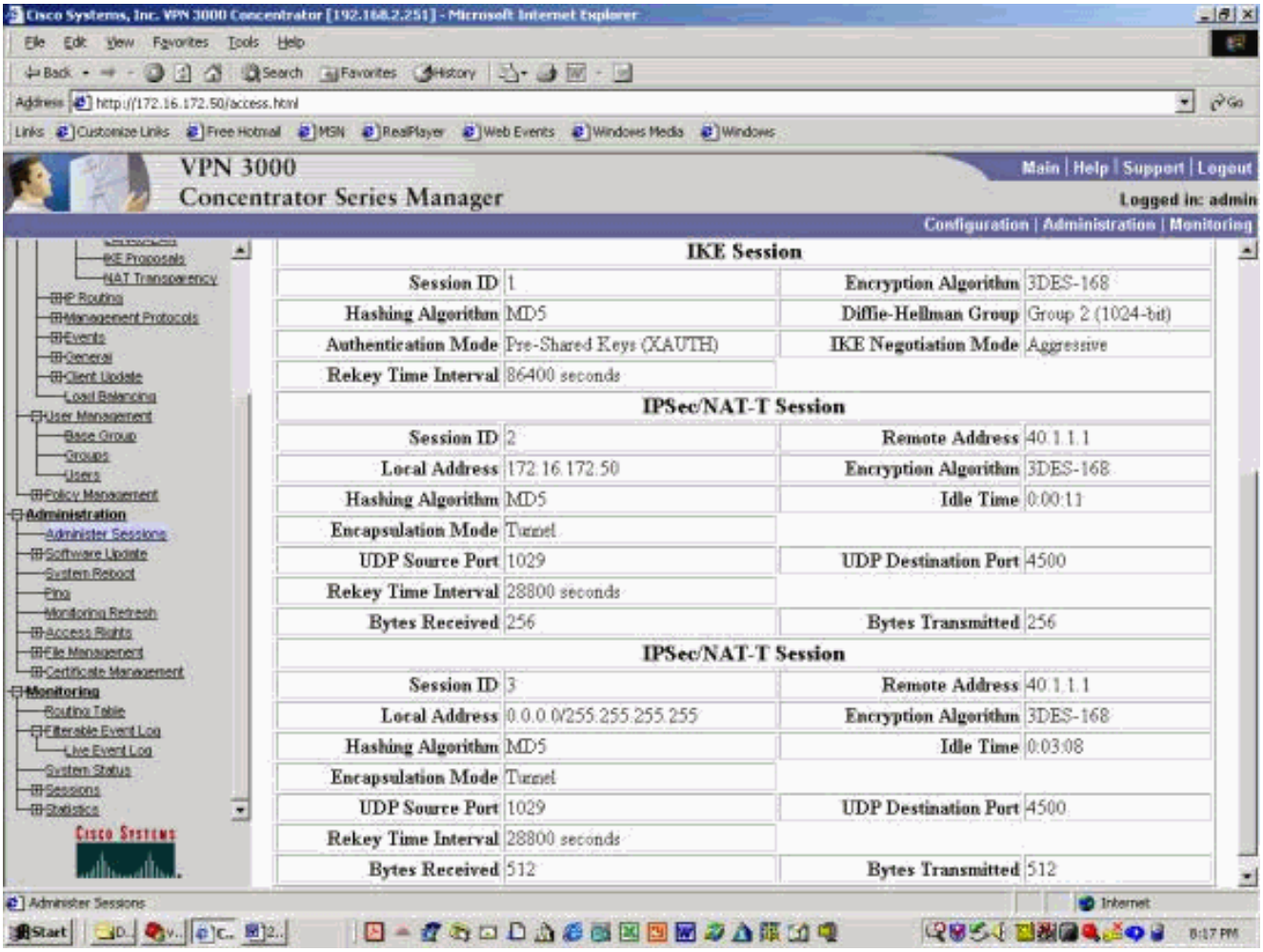
إحصائيات مركز الشبكة الخاصة الظاهرية (VPN)

أكمل الخطوات التالية:

1. على مركز الشبكة الخاصة الظاهرية (VPN)، أختر **إدارة > جلسة عمل المسؤول**.يمكن مشاهدة جلسة عمل عميل شبكة VPN ضمن جلسات عمل الوصول عن بعد. يوضح المثال التالي جلسات عمل الزبونين بعد أن قاما بإنشاء نفق IPSec للوصول إلى مركز الشبكة الخاصة الظاهرية (VPN). يستخدم كلا الجهازين عنوان IP العام 171.69.89.78 وتم تخصيصهما 40.1.1.1 و 40.1.1.2 على التوالي.



2. انقر نقرا مزدوجا فوق اسم مستخدم عميل.وترد إحصاءات IPSec/IKE، كما هو مبين في المثال التالي. ال UDP مصدر ميناء يستعمل ب الزبون 1029، والوجهة ميناء يستعمل 4500.



استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

ملاحظة: قبل إصدار أوامر **تصحيح الأخطاء**، راجع المعلومات المهمة في أوامر تصحيح الأخطاء.

ملاحظة: يمكن العثور على معلومات إضافية حول أستكشاف أخطاء PIX وإصلاحها في أستكشاف أخطاء أمان IP وإصلاحها - فهم أوامر تصحيح الأخطاء واستخدامها.

سجلات عميل شبكة VPN

على الكمبيوتر الشخصي الذي تم تثبيت عميل الشبكة الخاصة الظاهرية (VPN) عليه، افتح عارض السجل قبل إنشاء اتصال بموجه الشبكة الخاصة الظاهرية (VPN). يبرز إخراج السجل هذا الرسائل الخاصة ب NAT-T:

```
Sev=Info/6    DIALER/0x63300002  10/18/02  21:06:48.208      1
                                          .Initiating connection
Sev=Info/4    CM/0x63100002  10/18/02  21:06:48.218      2
                                       Begin connection process
Sev=Info/4    CM/0x63100004  10/18/02  21:06:48.218      3
                          Establish secure connection using Ethernet
Sev=Info/4    CM/0x63100026  10/18/02  21:06:48.218      4
                     "Attempt connection with server "172.16.172.50
Sev=Info/6  IKE/0x6300003B  10/18/02  21:07:42.326     42
 .Attempting to establish a connection with 172.16.172.50
Sev=Info/4  IKE/0x63000013  10/18/02  21:07:42.366     43
(SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID, VID, VID
```

```
                                                    to 172.16.172.50
      Sev=Info/5  IKE/0x6300002F  10/18/02  21:07:42.716     44
                                  Received ISAKMP packet: peer = 172.16.172.50
      Sev=Info/4  IKE/0x63000014  10/18/02  21:07:42.716     45
,RECEIVING <<< ISAKMP OAK AG (SA, KE, NON, ID, HASH, VID, VID, VID
                    VID, NAT-D, NAT-D, VID, VID) from 172.16.172.50
      Sev=Info/5  IKE/0x63000059  10/18/02  21:07:42.716     46
           Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100
      Sev=Info/5  IKE/0x63000001  10/18/02  21:07:42.716     47
                                  Peer is a Cisco-Unity compliant peer
      Sev=Info/5  IKE/0x63000059  10/18/02  21:07:42.716     48
                                  Vendor ID payload = 09002689DFD6B712
      Sev=Info/5  IKE/0x63000001  10/18/02  21:07:42.716     49
                                                    Peer supports XAUTH
      Sev=Info/5  IKE/0x63000059  10/18/02  21:07:42.716     50
           Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100
      Sev=Info/5  IKE/0x63000001  10/18/02  21:07:42.716     51
                                                      Peer supports DPD
      Sev=Info/5  IKE/0x63000059  10/18/02  21:07:42.716     52
           Vendor ID payload = 90CB80913EBB696E086381B5EC427B1F
      Sev=Info/5  IKE/0x63000001  10/18/02  21:07:42.716     53
                                                    Peer supports NAT-T
      Sev=Info/5  IKE/0x63000059  10/18/02  21:07:42.716     54
Vendor ID payload = 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
      Sev=Info/5  IKE/0x63000001  10/18/02  21:07:42.716     55
                                  Peer supports IKE fragmentation payloads
      Sev=Info/5  IKE/0x63000059  10/18/02  21:07:42.716     56
           Vendor ID payload = 1F07F70EAA6514D3B0FA96542A500306
      Sev=Info/4  IKE/0x63000013  10/18/02  21:07:42.757     57
,SENDING >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT, NAT-D
                                                    NAT-D) to 172.16.172.50
      Sev=Info/5  IKE/0x6300002F  10/18/02  21:07:42.767     58
                                  Received ISAKMP packet: peer = 172.16.172.50
      Sev=Info/4  IKE/0x63000014  10/18/02  21:07:42.767     59
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 172.16.172.50
       Sev=Info/4  CM/0x63100015  10/18/02  21:07:42.767     60
                                                    Launch xAuth application
  Sev=Info/4  IPSEC/0x63700014  10/18/02  21:07:42.967     61
                                                      Deleted all keys
       Sev=Info/4  CM/0x63100017  10/18/02  21:07:59.801     62
                                                 xAuth application returned
      Sev=Info/4  IKE/0x63000013  10/18/02  21:07:59.801     63
  SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.16.172.50
      Sev=Info/5  IKE/0x6300002F  10/18/02  21:08:00.101     64
                                  Received ISAKMP packet: peer = 172.16.172.50
      Sev=Info/4  IKE/0x63000014  10/18/02  21:08:00.101     65
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 172.16.172.50
      Sev=Info/5  IKE/0x63000071  10/18/02  21:08:00.101     66
                                            :Automatic NAT Detection Status
                                    Remote end is NOT behind a NAT device
                                      This end IS behind a NAT device
       Sev=Info/4  CM/0x6310000E  10/18/02  21:08:00.101     67
            Established Phase 1 SA.  1 Phase 1 SA in the system
      Sev=Info/4  IKE/0x63000013  10/18/02  21:08:00.111     68
  SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.16.172.50
      Sev=Info/5  IKE/0x6300005D  10/18/02  21:08:00.111     69
              Client sending a firewall request to concentrator
      Sev=Info/5  IKE/0x6300005C  10/18/02  21:08:00.111     70
 =Firewall Policy: Product=Cisco Integrated Client, Capability
                                        .(Centralized Protection Policy)
      Sev=Info/4  IKE/0x63000013  10/18/02  21:08:00.111     71
  SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.16.172.50
      Sev=Info/5  IKE/0x6300002F  10/18/02  21:08:00.122     72
                                  Received ISAKMP packet: peer = 172.16.172.50
```

```
                          Sev=Info/4  IKE/0x63000014  10/18/02  21:08:00.122     73
                  RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 172.16.172.50
                          Sev=Info/5  IKE/0x63000010  10/18/02  21:08:00.122     74
            MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: , value = 40.1.1.1
                          Sev=Info/5  IKE/0x6300000D  10/18/02  21:08:00.122     75
         MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value = 0x00000000
                          Sev=Info/5  IKE/0x6300000D  10/18/02  21:08:00.122     76
              MODE_CFG_REPLY: Attribute = MODECFG_UNITY_PFS: , value = 0x00000000
                          Sev=Info/5  IKE/0x6300000E  10/18/02  21:08:00.122     77
    .MODE_CFG_REPLY: Attribute = APPLICATION_VERSION, value = Cisco Systems, Inc
       VPN 3000 Concentrator Version 3.6.1.Rel built by vmurphy on Aug 29 2002/
                                                                    18:34:44
                          Sev=Info/5  IKE/0x6300000D  10/18/02  21:08:00.122     78
     = MODE_CFG_REPLY: Attribute = Recieved and using NAT-T port number , value
                                                                    0x00001194
                           Sev=Info/4  CM/0x63100019  10/18/02  21:08:00.132     79
                                                    Mode Config data received
                          Sev=Info/5  IKE/0x63000055  10/18/02  21:08:00.142     80
      = Received a key request from Driver for IP address 172.16.172.50, GW IP
                                                                    172.16.172.50
                          Sev=Info/4  IKE/0x63000013  10/18/02  21:08:00.142     81
              SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 172.16.172.50
                          Sev=Info/5  IKE/0x63000055  10/18/02  21:08:00.142     82
       = Received a key request from Driver for IP address 10.10.10.255, GW IP
                                                                    172.16.172.50
                          Sev=Info/4  IKE/0x63000013  10/18/02  21:08:00.142     83
              SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 172.16.172.50
                          Sev=Info/5  IKE/0x6300002F  10/18/02  21:08:00.172     84
                                       Received ISAKMP packet: peer = 172.16.172.50
                          Sev=Info/4  IKE/0x63000014  10/18/02  21:08:00.172     85
       RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:STATUS_RESP_LIFETIME) from
                                                                    172.16.172.50
                          Sev=Info/5  IKE/0x63000044  10/18/02  21:08:00.172     86
                               RESPONDER-LIFETIME notify has value of 86400 seconds
                          Sev=Info/5  IKE/0x63000046  10/18/02  21:08:00.172     87
        This SA has already been alive for 18 seconds, setting expiry to 86382
                                                          seconds from now
                          Sev=Info/5  IKE/0x6300002F  10/18/02  21:08:00.182     88
                                       Received ISAKMP packet: peer = 172.16.172.50
                          Sev=Info/4  IKE/0x63000014  10/18/02  21:08:00.182     89
(RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME
                                                          from 172.16.172.50
                          Sev=Info/5  IKE/0x63000044  10/18/02  21:08:00.182     90
                               RESPONDER-LIFETIME notify has value of 28800 seconds
                          Sev=Info/4  IKE/0x63000013  10/18/02  21:08:00.182     91
                                 SENDING >>> ISAKMP OAK QM *(HASH) to 172.16.172.50
                          Sev=Info/5  IKE/0x63000058  10/18/02  21:08:00.182     92
    Loading IPsec SA (Message ID = 0x347A7363 OUTBOUND SPI = 0x02CC3526 INBOUND
                                                          (SPI = 0x5BEEBB4C
                          Sev=Info/5  IKE/0x63000025  10/18/02  21:08:00.182     93
                                                    Loaded OUTBOUND ESP SPI: 0x02CC3526
                          Sev=Info/5  IKE/0x63000026  10/18/02  21:08:00.182     94
                                                    Loaded INBOUND ESP SPI: 0x5BEEBB4C
                           Sev=Info/4  CM/0x6310001A  10/18/02  21:08:00.182     95
                                                    One secure connection established
                      Sev=Info/6  DIALER/0x63300003  10/18/02  21:08:00.192     96
                                                          .Connection established
                          Sev=Info/5  IKE/0x6300002F  10/18/02  21:08:00.332     97
                                       Received ISAKMP packet: peer = 172.16.172.50
                          Sev=Info/4  IKE/0x63000014  10/18/02  21:08:00.332     98
(RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME
                                                          from 172.16.172.50
                          Sev=Info/5  IKE/0x63000044  10/18/02  21:08:00.332     99
                               RESPONDER-LIFETIME notify has value of 28800 seconds
```

```
Sev=Info/4           IKE/0x63000013  10/18/02  21:08:00.332    100
                  SENDING >>> ISAKMP OAK QM *(HASH) to 172.16.172.50
Sev=Info/5           IKE/0x63000058  10/18/02  21:08:00.342    101
Loading IPsec SA (Message ID = 0x2F81FB2D OUTBOUND SPI = 0x3316C6C9 INBOUND
                                                    (SPI = 0x6B96ED76
Sev=Info/5           IKE/0x63000025  10/18/02  21:08:00.342    102
                                    Loaded OUTBOUND ESP SPI: 0x3316C6C9
Sev=Info/5           IKE/0x63000026  10/18/02  21:08:00.342    103
                                    Loaded INBOUND ESP SPI: 0x6B96ED76
 Sev=Info/4           CM/0x63100022  10/18/02  21:08:00.342    104
                                    .Additional Phase 2 SA established
Sev=Info/4          IPSEC/0x63700014  10/18/02  21:08:01.203    105
                                                   Deleted all keys
Sev=Info/4          IPSEC/0x63700010  10/18/02  21:08:01.203    106
                                      Created a new key structure
Sev=Info/4          IPSEC/0x6370000F  10/18/02  21:08:01.203    107
                        Added key with SPI=0x2635cc02 into key list
Sev=Info/4          IPSEC/0x63700010  10/18/02  21:08:01.203    108
                                      Created a new key structure
Sev=Info/4          IPSEC/0x6370000F  10/18/02  21:08:01.203    109
                        Added key with SPI=0x4cbbee5b into key list
Sev=Info/4          IPSEC/0x63700010  10/18/02  21:08:01.203    110
                                      Created a new key structure
Sev=Info/4          IPSEC/0x6370000F  10/18/02  21:08:01.203    111
                        Added key with SPI=0xc9c61633 into key list
Sev=Info/4          IPSEC/0x63700010  10/18/02  21:08:01.203    112
                                      Created a new key structure
Sev=Info/4          IPSEC/0x6370000F  10/18/02  21:08:01.203    113
                        Added key with SPI=0x76ed966b into key list
Sev=Info/6           IKE/0x63000054  10/18/02  21:08:10.216    114
                                    Sent a ping on the Public IPSec SA
Sev=Info/4           IKE/0x63000013  10/18/02  21:08:20.381    115
SENDING >>> ISAKMP OAK INFO *(HASH, NOTIFY:HEARTBEAT) to 172.16.172.50
Sev=Info/6           IKE/0x63000052  10/18/02  21:08:20.381    116
                                        Sent a ping on the IKE SA
```

سجلات مركز VPN

لعرض السجلات الموجودة على مركز الشبكة الخاصة الظاهرية (VPN)، أختر **المراقبة > سجل الأحداث القابل للتصفية**، وحدد **فئات الأحداث IKE و iKEDBG و iKEDDECODE** و**IPSECDBG** التي لها مراحل خطورة من 1 إلى 13.

```
SEV=8 IKEDECODE/0 RPT=8190 171.69.89.78 20:22:42.390 10/20/2002 2835
                                    Exchange Type :Oakley Quick Mode
                                       ( Flags         :1   (ENCRYPT
                                            Message ID    : 1b050792
                                                  Length        : 52
  SEV=8 IKEDBG/0 RPT=9197 171.69.89.78 20:22:42.390 10/20/2002 2838
                  : RECEIVED Message (msgid=1b050792) with payloads
                                          (HDR + HASH (8) + NONE (0
                                                  total length : 48
   SEV=9 IKEDBG/0 RPT=9198 171.69.89.78 20:22:42.390 10/20/2002 2840
                                    [Group [ciscovpn] User [vpnclient2
                                                   processing hash
   SEV=9 IKEDBG/0 RPT=9199 171.69.89.78 20:22:42.390 10/20/2002 2841
                                    [Group [ciscovpn] User [vpnclient2
                                                loading all IPSEC SAs
   SEV=9 IKEDBG/1 RPT=793 171.69.89.78 20:22:42.390 10/20/2002 2842
                                    [Group [ciscovpn] User [vpnclient2
```

```
                                                    !Generating Quick Mode Key
                    SEV=9 IKEDBG/1 RPT=794 171.69.89.78 20:22:42.390 10/20/2002 2843
                                                [Group [ciscovpn] User [vpnclient2
                                                    !Generating Quick Mode Key
                      SEV=4 IKE/173 RPT=41 171.69.89.78 20:22:42.400 10/20/2002 2844
                                                [Group [ciscovpn] User [vpnclient2
                                          !NAT-Traversal successfully negotiated
                     .IPSec traffic will be encapsulated to pass through NAT devices
                   SEV=7 IKEDBG/0 RPT=9200 171.69.89.78 20:22:42.400 10/20/2002 2847
                                                [Group [ciscovpn] User [vpnclient2
                                                                :Loading host
                                                             Dst: 172.16.172.50
                                                              Src: 40.1.1.2
                       SEV=4 IKE/49 RPT=63 171.69.89.78 20:22:42.400 10/20/2002 2849
                                                [Group [ciscovpn] User [vpnclient2
                                    (Security negotiation complete for User (vpnclient2
                     Responder, Inbound SPI = 0x350f3cb1, Outbound SPI = 0xc74e30e5
                                  SEV=9 IPSECDBG/6 RPT=309 20:22:42.400 10/20/2002 2852
IPSEC key message parse - msgtype 1, Len 704, vers 1, pid 00000000, seq 0, err 0
type 2, mode 1, state 320, label 0, pad 0, spi c74e30e5, encrKeyLen 24, hashKe ,
 yLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 21, lifetime2 0, dsId
                                                                              0
                                SEV=9 IPSECDBG/1 RPT=1137 20:22:42.400 10/20/2002 2856
                                                    !Processing KEY_ADD msg
                                SEV=9 IPSECDBG/1 RPT=1138 20:22:42.400 10/20/2002 2857
                                                  key_msghdr2secassoc(): Enter
                                SEV=7 IPSECDBG/1 RPT=1139 20:22:42.400 10/20/2002 2858
                                                    No USER filter configured
                                SEV=9 IPSECDBG/1 RPT=1140 20:22:42.400 10/20/2002 2859
                                                      KeyProcessAdd: Enter
                                SEV=8 IPSECDBG/1 RPT=1141 20:22:42.400 10/20/2002 2860
                                                 KeyProcessAdd: Adding outbound SA
                                SEV=8 IPSECDBG/1 RPT=1142 20:22:42.400 10/20/2002 2861
          KeyProcessAdd: src 172.16.172.50 mask 0.0.0.0, DST 40.1.1.2 mask 0.0.0.0
                                SEV=8 IPSECDBG/1 RPT=1143 20:22:42.400 10/20/2002 2862
                                          KeyProcessAdd: FilterIpsecAddIkeSa success
                                 SEV=9 IPSECDBG/6 RPT=310 20:22:42.400 10/20/2002 2863
IPSEC key message parse - msgtype 3, Len 376, vers 1, pid 00000000, seq 0, err 0
type 2, mode 1, state 32, label 0, pad 0, spi 350f3cb1, encrKeyLen 24, hashKey ,
Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 21, lifetime2 0, dsId 0
                                SEV=9 IPSECDBG/1 RPT=1144 20:22:42.400 10/20/2002 2866
                                                  !Processing KEY_UPDATE MSG
                                SEV=9 IPSECDBG/1 RPT=1145 20:22:42.400 10/20/2002 2867
                                                   Update inbound SA addresses
                                SEV=9 IPSECDBG/1 RPT=1146 20:22:42.400 10/20/2002 2868
                                                  key_msghdr2secassoc(): Enter
                                SEV=7 IPSECDBG/1 RPT=1147 20:22:42.400 10/20/2002 2869
                                                    No USER filter configured
                                SEV=9 IPSECDBG/1 RPT=1148 20:22:42.400 10/20/2002 2870
                                                    KeyProcessUpdate: Enter
                                SEV=8 IPSECDBG/1 RPT=1149 20:22:42.400 10/20/2002 2871
                                                    KeyProcessUpdate: success
                                   SEV=8 IKEDBG/7 RPT=63 20:22:42.400 10/20/2002 2872
                                       IKE got a KEY_ADD MSG for SA: SPI = 0xc74e30e5
                                 SEV=8 IKEDBG/0 RPT=9201 20:22:42.400 10/20/2002 2873
                                            pitcher: rcv KEY_UPDATE, spi 0x350f3cb1
                     SEV=4 IKE/120 RPT=63 171.69.89.78 20:22:42.400 10/20/2002 2874
                                                [Group [ciscovpn] User [vpnclient2
                                                (PHASE 2 COMPLETED (msgid=1b050792
               SEV=8 IKEDECODE/0 RPT=8191 171.69.89.78 20:22:42.430 10/20/2002 2875
                                              ( ISAKMP HEADER : ( Version 1.0
                                    Initiator Cookie(8): C5 A0 F0 8B 69 60 D7 47
                                    Responder Cookie(8): 48 65 B1 6F 36 1F 9D 3A
                                                (Next Payload  :HASH (8
```

```
                                                Exchange Type :Oakley Quick Mode
                                                   ( Flags         :1   (ENCRYPT
                                                        Message ID    : cf9d1420
                                                              Length        : 52
                SEV=8 IKEDBG/0 RPT=9202 171.69.89.78 20:22:42.430 10/20/2002 2882
                                : RECEIVED Message (msgid=cf9d1420) with payloads
                                                         (HDR + HASH (8) + NONE (0
                                                               total length : 48
                SEV=9 IKEDBG/0 RPT=9203 171.69.89.78 20:22:42.430 10/20/2002 2884
                                                [Group [ciscovpn] User [vpnclient2
                                                          processing hash

                SEV=9 IKEDBG/0 RPT=9204 171.69.89.78 20:22:42.430 10/20/2002 2885
                                                [Group [ciscovpn] User [vpnclient2
                                                       loading all IPSEC SAs
                 SEV=9 IKEDBG/1 RPT=795 171.69.89.78 20:22:42.430 10/20/2002 2886
                                                [Group [ciscovpn] User [vpnclient2
                                                        !Generating Quick Mode Key
                 SEV=9 IKEDBG/1 RPT=796 171.69.89.78 20:22:42.440 10/20/2002 2887
                                                [Group [ciscovpn] User [vpnclient2
                                                        !Generating Quick Mode Key
                   SEV=4 IKE/173 RPT=42 171.69.89.78 20:22:42.440 10/20/2002 2888
                                                [Group [ciscovpn] User [vpnclient2
                                             !NAT-Traversal successfully negotiated
                  .IPSec traffic will be encapsulated to pass through NAT devices
                SEV=7 IKEDBG/0 RPT=9205 171.69.89.78 20:22:42.440 10/20/2002 2891
                                                [Group [ciscovpn] User [vpnclient2
                                                                :Loading subnet
                                                    DST: 0.0.0.0  mask: 0.0.0.0
                                                                Src: 40.1.1.2
                    SEV=4 IKE/49 RPT=64 171.69.89.78 20:22:42.440 10/20/2002 2893
                                                [Group [ciscovpn] User [vpnclient2
                                       (Security negotiation complete for User (vpnclient2
                   Responder, Inbound SPI = 0x2a2e2dcd, Outbound SPI = 0xf1f4d328
                                    SEV=9 IPSECDBG/6 RPT=311 20:22:42.440 10/20/2002 2896
IPSEC key message parse - msgtype 1, Len 704, vers 1, pid 00000000, seq 0, err 0
type 2, mode 1, state 320, label 0, pad 0, spi f1f4d328, encrKeyLen 24, hashKe ,
 yLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 21, lifetime2 0, dsId
                                                                              0
                                    SEV=9 IPSECDBG/1 RPT=1150 20:22:42.440 10/20/2002 2900
                                                          !Processing KEY_ADD MSG
                                    SEV=9 IPSECDBG/1 RPT=1151 20:22:42.440 10/20/2002 2901
                                                       key_msghdr2secassoc(): Enter
                                    SEV=7 IPSECDBG/1 RPT=1152 20:22:42.440 10/20/2002 2902
                                                         No USER filter configured
                                    SEV=9 IPSECDBG/1 RPT=1153 20:22:42.440 10/20/2002 2903
                                                            KeyProcessAdd: Enter
                                    SEV=8 IPSECDBG/1 RPT=1154 20:22:42.440 10/20/2002 2904
                                                     KeyProcessAdd: Adding outbound SA
                                    SEV=8 IPSECDBG/1 RPT=1155 20:22:42.440 10/20/2002 2905
      KeyProcessAdd: src 0.0.0.0 mask 255.255.255.255, DST 40.1.1.2 mask 0.0.0.0
                                    SEV=8 IPSECDBG/1 RPT=1156 20:22:42.440 10/20/2002 2906
                                                KeyProcessAdd: FilterIpsecAddIkeSa success
                                     SEV=9 IPSECDBG/6 RPT=312 20:22:42.440 10/20/2002 2907
IPSEC key message parse - msgtype 3, Len 376, vers 1, pid 00000000, seq 0, err 0
type 2, mode 1, state 32, label 0, pad 0, spi 2a2e2dcd, encrKeyLen 24, hashKey ,
Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 21, lifetime2 0, dsId 0
                                    SEV=9 IPSECDBG/1 RPT=1157 20:22:42.440 10/20/2002 2910
                                                          !Processing KEY_UPDATE MSG
                                    SEV=9 IPSECDBG/1 RPT=1158 20:22:42.440 10/20/2002 2911
                                                       Update inbound SA addresses
                                    SEV=9 IPSECDBG/1 RPT=1159 20:22:42.440 10/20/2002 2912
                                                       key_msghdr2secassoc(): Enter
                                    SEV=7 IPSECDBG/1 RPT=1160 20:22:42.440 10/20/2002 2913
```

```
                                                  No USER filter configured
                          SEV=9 IPSECDBG/1 RPT=1161 20:22:42.440 10/20/2002 2914
                                                    KeyProcessUpdate: Enter
                          SEV=8 IPSECDBG/1 RPT=1162 20:22:42.440 10/20/2002 2915
                                                  KeyProcessUpdate: success
                              SEV=8 IKEDBG/7 RPT=64 20:22:42.440 10/20/2002 2916
                                  IKE got a KEY_ADD MSG for SA: SPI = 0xf1f4d328
                                SEV=8 IKEDBG/0 RPT=9206 20:22:42.440 10/20/2002 2917
                                               pitcher: rcv KEY_UPDATE, spi 0x2a2e2dcd
                     SEV=4 IKE/120 RPT=64 171.69.89.78 20:22:42.440 10/20/2002 2918
                                            [Group [ciscovpn] User [vpnclient2
                                            (PHASE 2 COMPLETED (msgid=cf9d1420
                          SEV=7 IPSECDBG/1 RPT=1163 20:22:44.680 10/20/2002 2919
                                           !IPSec Inbound SA has received data
                                SEV=8 IKEDBG/0 RPT=9207 20:22:44.680 10/20/2002 2920
                                                 pitcher: recv KEY_SA_ACTIVE spi 0x2a2e2dcd
                                SEV=8 IKEDBG/0 RPT=9208 20:22:44.680 10/20/2002 2921
KEY_SA_ACTIVE no old rekey centry found with new spi 0x2a2e2dcd, mess_id 0x0
                   SEV=9 IPSECDBG/18 RPT=828 171.69.89.78 20:22:47.530 10/20/2002 2922
                                  Xmit IPSEC-over-UDP NAT keepalive packet: success
                   SEV=9 IPSECDBG/18 RPT=829 171.69.89.78 20:22:47.530 10/20/2002 2923
                                  Xmit IPSEC-over-UDP NAT keepalive packet: success
                          SEV=9 IPSECDBG/17 RPT=668 20:22:48.280 10/20/2002 2924
                                  Received an IPSEC-over-NAT-T NAT keepalive packet
                          SEV=9 IPSECDBG/17 RPT=669 20:22:52.390 10/20/2002 2925
                                  Received an IPSEC-over-NAT-T NAT keepalive packet
                          SEV=7 IPSECDBG/1 RPT=1164 20:22:52.720 10/20/2002 2926
                                           !IPSec Inbound SA has received data
                                SEV=8 IKEDBG/0 RPT=9209 20:22:52.720 10/20/2002 2927
                                                 pitcher: recv KEY_SA_ACTIVE spi 0x19fb2d12
                                SEV=8 IKEDBG/0 RPT=9210 20:22:52.720 10/20/2002 2928
KEY_SA_ACTIVE no old rekey centry found with new spi 0x19fb2d12, mess_id 0x0
                   SEV=9 IPSECDBG/18 RPT=830 171.69.89.78 20:22:56.530 10/20/2002 2929
                                  Xmit IPSEC-over-UDP NAT keepalive packet: success
                   SEV=9 IPSECDBG/18 RPT=831 171.69.89.78 20:22:56.530 10/20/2002 2930
                                  Xmit IPSEC-over-UDP NAT keepalive packet: success
                 SEV=8 IKEDECODE/0 RPT=8192 171.69.89.78 20:22:58.300 10/20/2002 2931
                                              ( ISAKMP HEADER : ( Version 1.0
                                    Initiator Cookie(8): B6 92 24 F4 96 0A 2D 9E
                                    Responder Cookie(8): 76 FE F6 55 1F 9D 49 F3
                                                   (Next Payload  :HASH (8
                                           Exchange Type :Oakley Informational
                                                ( Flags         :1   (ENCRYPT
                                                     Message ID    : d4a0ec25
                                                          Length        : 76
                     SEV=8 IKEDBG/0 RPT=9211 171.69.89.78 20:22:58.300 10/20/2002 2938
                                    : RECEIVED Message (msgid=d4a0ec25) with payloads
                                           (HDR + HASH (8) + NOTIFY (11) + NONE (0
                                                             total length : 76
                     SEV=9 IKEDBG/0 RPT=9212 171.69.89.78 20:22:58.300 10/20/2002 2940
                                              [Group [ciscovpn] User [vpnclient1
                                                               processing hash
                     SEV=9 IKEDBG/0 RPT=9213 171.69.89.78 20:22:58.300 10/20/2002 2941
                                              [Group [ciscovpn] User [vpnclient1
                                                                Processing Notify payload
                 SEV=8 IKEDECODE/0 RPT=8193 171.69.89.78 20:22:58.300 10/20/2002 2942
                                                             : Notify Payload Decode
                                                           (DOI           :IPSEC (1
                                                          (Protocol      :ISAKMP (1
                                                 (Message       :Altiga keep-alive (40500
                      Spi           :B6 92 24 F4 96 0A 2D 9E 76 FE F6 55 1F 9D 49 F3
                                                               Length        :28
                     SEV=9 IKEDBG/41 RPT=336 171.69.89.78 20:22:58.300 10/20/2002 2948
                                              [Group [ciscovpn] User [vpnclient1
```

```
Received keep-alive of type Altiga keep-alive, not the negotiated type
  SEV=8 IKEDECODE/0 RPT=8194 171.69.89.78 20:22:58.310 10/20/2002 2950
                                        ( ISAKMP HEADER : ( Version 1.0
                          Initiator Cookie(8): B6 92 24 F4 96 0A 2D 9E
                          Responder Cookie(8): 76 FE F6 55 1F 9D 49 F3
                                             (Next Payload  :HASH (8
                                  Exchange Type :Oakley Informational
                                        ( Flags         :1   (ENCRYPT
                                             Message ID    : d196c721
                                                   Length        : 84
     SEV=8 IKEDBG/0 RPT=9214 171.69.89.78 20:22:58.310 10/20/2002 2957
                       : RECEIVED Message (msgid=d196c721) with payloads
                                  (HDR + HASH (8) + NOTIFY (11) + NONE (0
                                                     total length : 80
     SEV=9 IKEDBG/0 RPT=9215 171.69.89.78 20:22:58.310 10/20/2002 2959
                                       [Group [ciscovpn] User [vpnclient1
                                                       processing hash
     SEV=9 IKEDBG/0 RPT=9216 171.69.89.78 20:22:58.310 10/20/2002 2960
                                       [Group [ciscovpn] User [vpnclient1
                                                 Processing Notify payload
  SEV=8 IKEDECODE/0 RPT=8195 171.69.89.78 20:22:58.310 10/20/2002 2961
                                                 : Notify Payload Decode
                                              (DOI           :IPSEC (1
                                             (Protocol      :ISAKMP (1
                                  (Message       :DPD R-U-THERE (36136
      Spi           :B6 92 24 F4 96 0A 2D 9E 76 FE F6 55 1F 9D 49 F3
                                                   Length        :32
      SEV=9 IKEDBG/36 RPT=92 171.69.89.78 20:22:58.310 10/20/2002 2967
                                       [Group [ciscovpn] User [vpnclient1
  (Sending keep-alive of type DPD R-U-THERE-ACK (seq number 0x2d932552
     SEV=9 IKEDBG/0 RPT=9217 171.69.89.78 20:22:58.310 10/20/2002 2969
                                       [Group [ciscovpn] User [vpnclient1
                                                  constructing blank hash
     SEV=9 IKEDBG/0 RPT=9218 171.69.89.78 20:22:58.310 10/20/2002 2970
                                       [Group [ciscovpn] User [vpnclient1
                                                    constructing qm hash
     SEV=8 IKEDBG/0 RPT=9219 171.69.89.78 20:22:58.310 10/20/2002 2971
                          : SENDING Message (msgid=d678099) with payloads
                                             (HDR + HASH (8) + NOTIFY (11
                                                     total length : 80
  SEV=8 IKEDECODE/0 RPT=8196 171.69.89.78 20:23:02.400 10/20/2002 2973
                                        ( ISAKMP HEADER : ( Version 1.0
                          Initiator Cookie(8): C5 A0 F0 8B 69 60 D7 47
                          Responder Cookie(8): 48 65 B1 6F 36 1F 9D 3A
                                             (Next Payload  :HASH (8
                                  Exchange Type :Oakley Informational
                                        ( Flags         :1   (ENCRYPT
                                             Message ID    : 317b646a
                                                   Length        : 76
     SEV=8 IKEDBG/0 RPT=9220 171.69.89.78 20:23:02.400 10/20/2002 2980
                       : RECEIVED Message (msgid=317b646a) with payloads
                                  (HDR + HASH (8) + NOTIFY (11) + NONE (0
                                                     total length : 76
     SEV=9 IKEDBG/0 RPT=9221 171.69.89.78 20:23:02.400 10/20/2002 2982
                                       [Group [ciscovpn] User [vpnclient2
                                                       processing hash
     SEV=9 IKEDBG/0 RPT=9222 171.69.89.78 20:23:02.400 10/20/2002 2983
                                       [Group [ciscovpn] User [vpnclient2
                                                 Processing Notify payload
  SEV=8 IKEDECODE/0 RPT=8197 171.69.89.78 20:23:02.400 10/20/2002 2984
                                                 : Notify Payload Decode
                                              (DOI           :IPSEC (1
                                             (Protocol      :ISAKMP (1
                                  (Message       :Altiga keep-alive (40500
```

```
      Spi           :C5 A0 F0 8B 69 60 D7 47 48 65 B1 6F 36 1F 9D 3A
                                                  Length        :28
     SEV=9 IKEDBG/41 RPT=337 171.69.89.78 20:23:02.400 10/20/2002 2990
                                       [Group [ciscovpn] User [vpnclient2
Received keep-alive of type Altiga keep-alive, not the negotiated type
                SEV=9 IPSECDBG/17 RPT=670 20:23:02.410 10/20/2002 2992
                     Received an IPSEC-over-NAT-T NAT keepalive packet
   SEV=9 IPSECDBG/18 RPT=832 171.69.89.78 20:23:05.530 10/20/2002 2993
                     Xmit IPSEC-over-UDP NAT keepalive packet: success
   SEV=9 IPSECDBG/18 RPT=833 171.69.89.78 20:23:05.530 10/20/2002 2994
                     Xmit IPSEC-over-UDP NAT keepalive packet: success
                SEV=9 IPSECDBG/17 RPT=671 20:23:08.310 10/20/2002 2995
                     Received an IPSEC-over-NAT-T NAT keepalive packet
                SEV=9 IPSECDBG/17 RPT=672 20:23:12.420 10/20/2002 2996
                     Received an IPSEC-over-NAT-T NAT keepalive packet
   SEV=9 IPSECDBG/18 RPT=834 171.69.89.78 20:23:14.530 10/20/2002 2997
                     Xmit IPSEC-over-UDP NAT keepalive packet: success
   SEV=9 IPSECDBG/18 RPT=835 171.69.89.78 20:23:14.530 10/20/2002 2998
                     Xmit IPSEC-over-UDP NAT keepalive packet: success
  SEV=8 IKEDECODE/0 RPT=8198 171.69.89.78 20:23:18.330 10/20/2002 2999
                                       ( ISAKMP HEADER : ( Version 1.0
                        Initiator Cookie(8): B6 92 24 F4 96 0A 2D 9E
                        Responder Cookie(8): 76 FE F6 55 1F 9D 49 F3
                                            (Next Payload  :HASH (8
                                  Exchange Type :Oakley Informational
                                       ( Flags         :1   (ENCRYPT
                                            Message ID    : f6457474
                                                  Length        : 76
     SEV=8 IKEDBG/0 RPT=9223 171.69.89.78 20:23:18.330 10/20/2002 3006
                     : RECEIVED Message (msgid=f6457474) with payloads
                               (HDR + HASH (8) + NOTIFY (11) + NONE (0
                                                    total length : 76
     SEV=9 IKEDBG/0 RPT=9224 171.69.89.78 20:23:18.330 10/20/2002 3008
                                       [Group [ciscovpn] User [vpnclient1
                                                      processing hash
     SEV=9 IKEDBG/0 RPT=9225 171.69.89.78 20:23:18.330 10/20/2002 3009
                                       [Group [ciscovpn] User [vpnclient1
                                                Processing Notify payload
  SEV=8 IKEDECODE/0 RPT=8199 171.69.89.78 20:23:18.330 10/20/2002 3010
                                                  : Notify Payload Decode
                                             (DOI           :IPSEC (1
                                            (Protocol      :ISAKMP (1
                                 (Message       :Altiga keep-alive (40500
      Spi           :B6 92 24 F4 96 0A 2D 9E 76 FE F6 55 1F 9D 49 F3
                                                  Length        :28
     SEV=9 IKEDBG/41 RPT=338 171.69.89.78 20:23:18.330 10/20/2002 3016
                                       [Group [ciscovpn] User [vpnclient1
Received keep-alive of type Altiga keep-alive, not the negotiated type
                SEV=9 IPSECDBG/17 RPT=673 20:23:18.330 10/20/2002 3018
                     Received an IPSEC-over-NAT-T NAT keepalive packet
  SEV=8 IKEDECODE/0 RPT=8200 171.69.89.78 20:23:22.430 10/20/2002 3019
                                       ( ISAKMP HEADER : ( Version 1.0
                        Initiator Cookie(8): C5 A0 F0 8B 69 60 D7 47
                        Responder Cookie(8): 48 65 B1 6F 36 1F 9D 3A
                                            (Next Payload  :HASH (8
                                  Exchange Type :Oakley Informational
                                       ( Flags         :1   (ENCRYPT
                                            Message ID    : 358ae39e
                                                  Length        : 76
     SEV=8 IKEDBG/0 RPT=9226 171.69.89.78 20:23:22.430 10/20/2002 3026
                     : RECEIVED Message (msgid=358ae39e) with payloads
                               (HDR + HASH (8) + NOTIFY (11) + NONE (0
                                                    total length : 76
     SEV=9 IKEDBG/0 RPT=9227 171.69.89.78 20:23:22.430 10/20/2002 3028
```

```
                                        [Group [ciscovpn] User [vpnclient2
                                                               processing hash
    SEV=9 IKEDBG/0 RPT=9228 171.69.89.78 20:23:22.430 10/20/2002 3029
                                        [Group [ciscovpn] User [vpnclient2
                                                 Processing Notify payload
  SEV=8 IKEDECODE/0 RPT=8201 171.69.89.78 20:23:22.430 10/20/2002 3030
                                                    : Notify Payload Decode
                                               (DOI           :IPSEC (1
                                              (Protocol      :ISAKMP (1
                              (Message       :Altiga keep-alive (40500
     Spi           :C5 A0 F0 8B 69 60 D7 47 48 65 B1 6F 36 1F 9D 3A
                                                    Length        :28
    SEV=9 IKEDBG/41 RPT=339 171.69.89.78 20:23:22.430 10/20/2002 3036
                                        [Group [ciscovpn] User [vpnclient2
Received keep-alive of type Altiga keep-alive, not the negotiated type
                SEV=9 IPSECDBG/17 RPT=674 20:23:22.430 10/20/2002 3038
                     Received an IPSEC-over-NAT-T NAT keepalive packet
   SEV=9 IPSECDBG/18 RPT=836 171.69.89.78 20:23:23.530 10/20/2002 3039
                     Xmit IPSEC-over-UDP NAT keepalive packet: success
   SEV=9 IPSECDBG/18 RPT=837 171.69.89.78 20:23:23.530 10/20/2002 3040
                     Xmit IPSEC-over-UDP NAT keepalive packet: success
                SEV=9 IPSECDBG/17 RPT=675 20:23:28.340 10/20/2002 3041
                     Received an IPSEC-over-NAT-T NAT keepalive packet
                SEV=9 IPSECDBG/17 RPT=676 20:23:32.440 10/20/2002 3042
                     Received an IPSEC-over-NAT-T NAT keepalive packet
   SEV=9 IPSECDBG/18 RPT=838 171.69.89.78 20:23:32.530 10/20/2002 3043
                     Xmit IPSEC-over-UDP NAT keepalive packet: success
   SEV=9 IPSECDBG/18 RPT=839 171.69.89.78 20:23:32.530 10/20/2002 3044
                     Xmit IPSEC-over-UDP NAT keepalive packet: success
  SEV=8 IKEDECODE/0 RPT=8202 171.69.89.78 20:23:38.360 10/20/2002 3045
                                     ( ISAKMP HEADER : ( Version 1.0
                        Initiator Cookie(8): B6 92 24 F4 96 0A 2D 9E
                        Responder Cookie(8): 76 FE F6 55 1F 9D 49 F3
                                      (Next Payload  :HASH (8
                                Exchange Type :Oakley Informational
                                     ( Flags         :1   (ENCRYPT
                                          Message ID    : fa8597e6
                                               Length        : 76
    SEV=8 IKEDBG/0 RPT=9229 171.69.89.78 20:23:38.360 10/20/2002 3052
                     : RECEIVED Message (msgid=fa8597e6) with payloads
                               (HDR + HASH (8) + NOTIFY (11) + NONE (0
                                                  total length : 76
    SEV=9 IKEDBG/0 RPT=9230 171.69.89.78 20:23:38.360 10/20/2002 3054
                                        [Group [ciscovpn] User [vpnclient1
                                                               processing hash
    SEV=9 IKEDBG/0 RPT=9231 171.69.89.78 20:23:38.360 10/20/2002 3055
                                        [Group [ciscovpn] User [vpnclient1
                                                 Processing Notify payload
  SEV=8 IKEDECODE/0 RPT=8203 171.69.89.78 20:23:38.360 10/20/2002 3056
                                                    : Notify Payload Decode
                                               (DOI           :IPSEC (1
                                              (Protocol      :ISAKMP (1
                              (Message       :Altiga keep-alive (40500
     Spi           :B6 92 24 F4 96 0A 2D 9E 76 FE F6 55 1F 9D 49 F3
                                                    Length        :28
    SEV=9 IKEDBG/41 RPT=340 171.69.89.78 20:23:38.360 10/20/2002 3062
                                        [Group [ciscovpn] User [vpnclient1
Received keep-alive of type Altiga keep-alive, not the negotiated type
                SEV=9 IPSECDBG/17 RPT=677 20:23:38.360 10/20/2002 3064
                     Received an IPSEC-over-NAT-T NAT keepalive packet
   SEV=9 IPSECDBG/18 RPT=840 171.69.89.78 20:23:41.530 10/20/2002 3065
                     Xmit IPSEC-over-UDP NAT keepalive packet: success
   SEV=9 IPSECDBG/18 RPT=841 171.69.89.78 20:23:41.530 10/20/2002 3066
                     Xmit IPSEC-over-UDP NAT keepalive packet: success
```

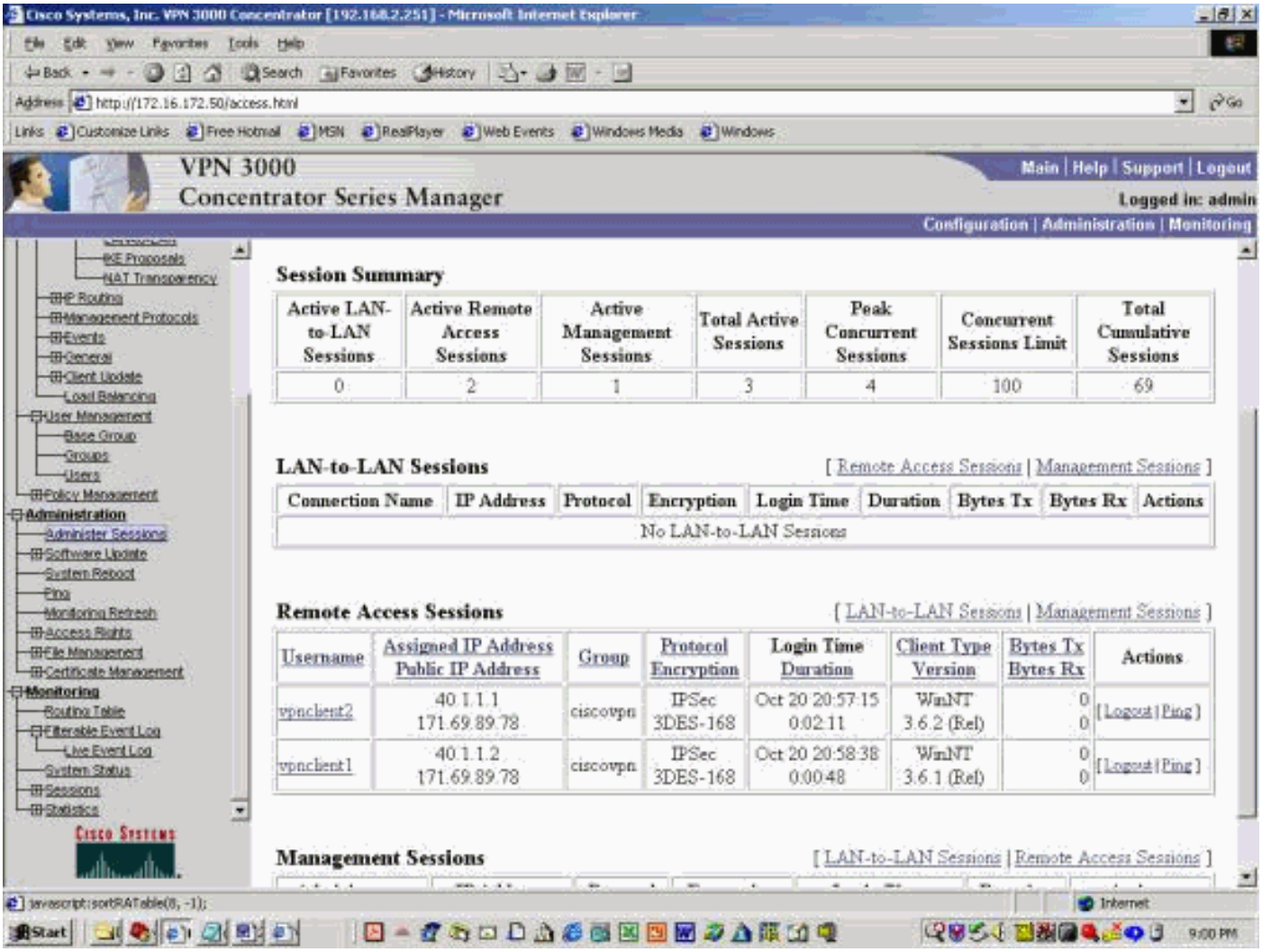
```
SEV=8 IKEDECODE/0 RPT=8204 171.69.89.78 20:23:42.470 10/20/2002 3067
                                        ( ISAKMP HEADER : ( Version 1.0
                            Initiator Cookie(8): C5 A0 F0 8B 69 60 D7 47
                            Responder Cookie(8): 48 65 B1 6F 36 1F 9D 3A
                                                 (Next Payload  :HASH (8
                                      Exchange Type :Oakley Informational
                                                 ( Flags         :1   (ENCRYPT
SEV=8 IKEDECODE/0 RPT=8204 171.69.89.78 20:23:42.470 10/20/2002 3073
                                               Message ID    : c892dd4c
                                                     Length        : 76
                          : RECEIVED Message (msgid=c892dd4c) with payloads
                                    (HDR + HASH (8) + NOTIFY (11) + NONE (0
                                                       total length : 76
   SEV=9 IKEDBG/0 RPT=9233 171.69.89.78 20:23:42.470 10/20/2002 3076
                                        [Group [ciscovpn] User [vpnclient2
                                                         processing hash
   SEV=9 IKEDBG/0 RPT=9234 171.69.89.78 20:23:42.470 10/20/2002 3077
                                        [Group [ciscovpn] User [vpnclient2
                                                  Processing Notify payload
SEV=8 IKEDECODE/0 RPT=8205 171.69.89.78 20:23:42.470 10/20/2002 3078
                                                    : Notify Payload Decode
                                                 (DOI           :IPSEC (1
                                                (Protocol      :ISAKMP (1
                                    (Message       :Altiga keep-alive (40500
    Spi           :C5 A0 F0 8B 69 60 D7 47 48 65 B1 6F 36 1F 9D 3A
                                                      Length        :28
   SEV=9 IKEDBG/41 RPT=341 171.69.89.78 20:23:42.470 10/20/2002 3084
                                        [Group [ciscovpn] User [vpnclient2
Received keep-alive of type Altiga keep-alive, not the negotiated type
                SEV=9 IPSECDBG/17 RPT=678 20:23:42.470 10/20/2002 3086
                                     Received an IPSEC-over-NAT-T NAT keepalive packet
                SEV=9 IPSECDBG/17 RPT=679 20:23:48.370 10/20/2002 3087
                                     Received an IPSEC-over-NAT-T NAT keepalive packet
  SEV=9 IPSECDBG/18 RPT=842 171.69.89.78 20:23:50.530 10/20/2002 3088
                                     Xmit IPSEC-over-UDP NAT keepalive packet: success
  SEV=9 IPSECDBG/18 RPT=843 171.69.89.78 20:23:50.530 10/20/2002 3089
                                     Xmit IPSEC-over-UDP NAT keepalive packet: success
                SEV=9 IPSECDBG/17 RPT=680 20:23:52.470 10/20/2002 3090
                                     Received an IPSEC-over-NAT-T NAT keepalive packet
SEV=8 IKEDECODE/0 RPT=8206 171.69.89.78 20:23:58.380 10/20/2002 3091
                                        ( ISAKMP HEADER : ( Version 1.0
                            Initiator Cookie(8): B6 92 24 F4 96 0A 2D 9E
                            Responder Cookie(8): 76 FE F6 55 1F 9D 49 F3
                                                 (Next Payload  :HASH (8
                                      Exchange Type :Oakley Informational
                                                 ( Flags         :1   (ENCRYPT
                                               Message ID    : 943c7d99
                                                     Length        : 76
   SEV=8 IKEDBG/0 RPT=9235 171.69.89.78 20:23:58.390 10/20/2002 3098
                          : RECEIVED Message (msgid=943c7d99) with payloads
                                    (HDR + HASH (8) + NOTIFY (11) + NONE (0
                                                       total length : 76
   SEV=9 IKEDBG/0 RPT=9236 171.69.89.78 20:23:58.390 10/20/2002 3100
                                        [Group [ciscovpn] User [vpnclient1
                                                         processing hash
   SEV=9 IKEDBG/0 RPT=9237 171.69.89.78 20:23:58.390 10/20/2002 3101
                                        [Group [ciscovpn] User [vpnclient1
                                                  Processing Notify payload
SEV=8 IKEDECODE/0 RPT=8207 171.69.89.78 20:23:58.390 10/20/2002 3102
                                                    : Notify Payload Decode
                                                 (DOI           :IPSEC (1
                                                (Protocol      :ISAKMP (1
                                    (Message       :Altiga keep-alive (40500
    Spi           :B6 92 24 F4 96 0A 2D 9E 76 FE F6 55 1F 9D 49 F3
```

```
                                                    Length       :28
SEV=9 IKEDBG/41 RPT=342 171.69.89.78 20:23:58.390 10/20/2002 3108
                                                [Group [ciscovpn] User [vpnclient1
Received keep-alive of type Altiga keep-alive, not the negotiated type
SEV=9 IPSECDBG/17 RPT=681 20:23:58.390 10/20/2002 3110
                                    Received an IPSEC-over-NAT-T NAT keepalive packet
SEV=9 IPSECDBG/18 RPT=844 171.69.89.78 20:23:59.530 10/20/2002 3111
                                    Xmit IPSEC-over-UDP NAT keepalive packet: success
SEV=9 IPSECDBG/18 RPT=845 171.69.89.78 20:23:59.530 10/20/2002 3112
                                    Xmit IPSEC-over-UDP NAT keepalive packet: success
```

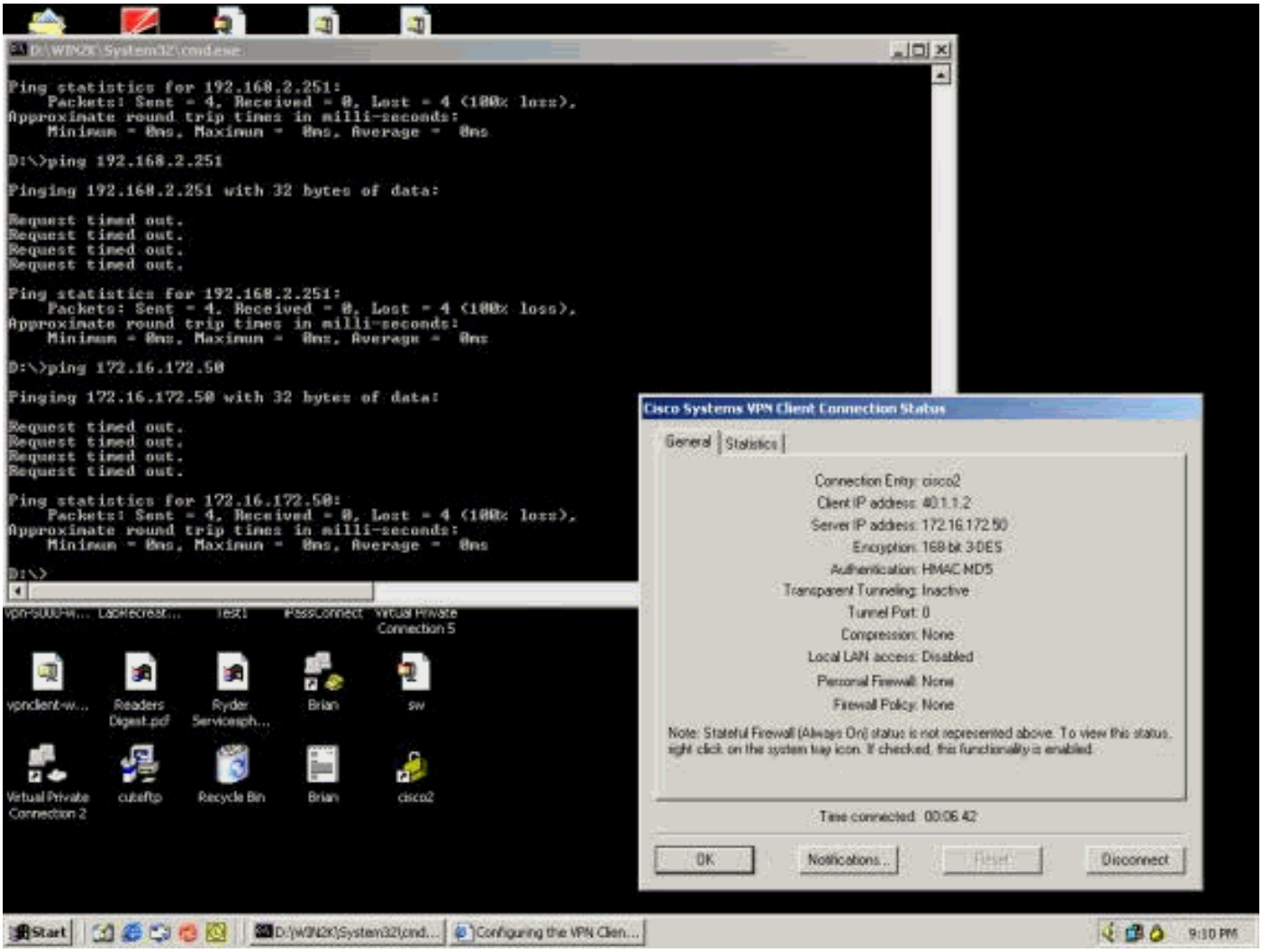
أستكشاف الأخطاء وإصلاحها بشكل إضافي

يتضمن NAT-T حركة مرور IPSec في مخططات بيانات UDP باستخدام المنفذ 4500. إذا لم يتم التحقق من NAT-T على مركز VPN أو إذا لم يتم التحقق من شفافية NAT على عميل VPN، يتم إنشاء نفق IPSec، ومع ذلك، لا يمكنك تمرير أي بيانات. ل NAT-T أن يعمل، أنت ينبغي جعلت ال NAT-T فحصت على المركز و NAT شفافية (على UDP) فحصت على الزبون.

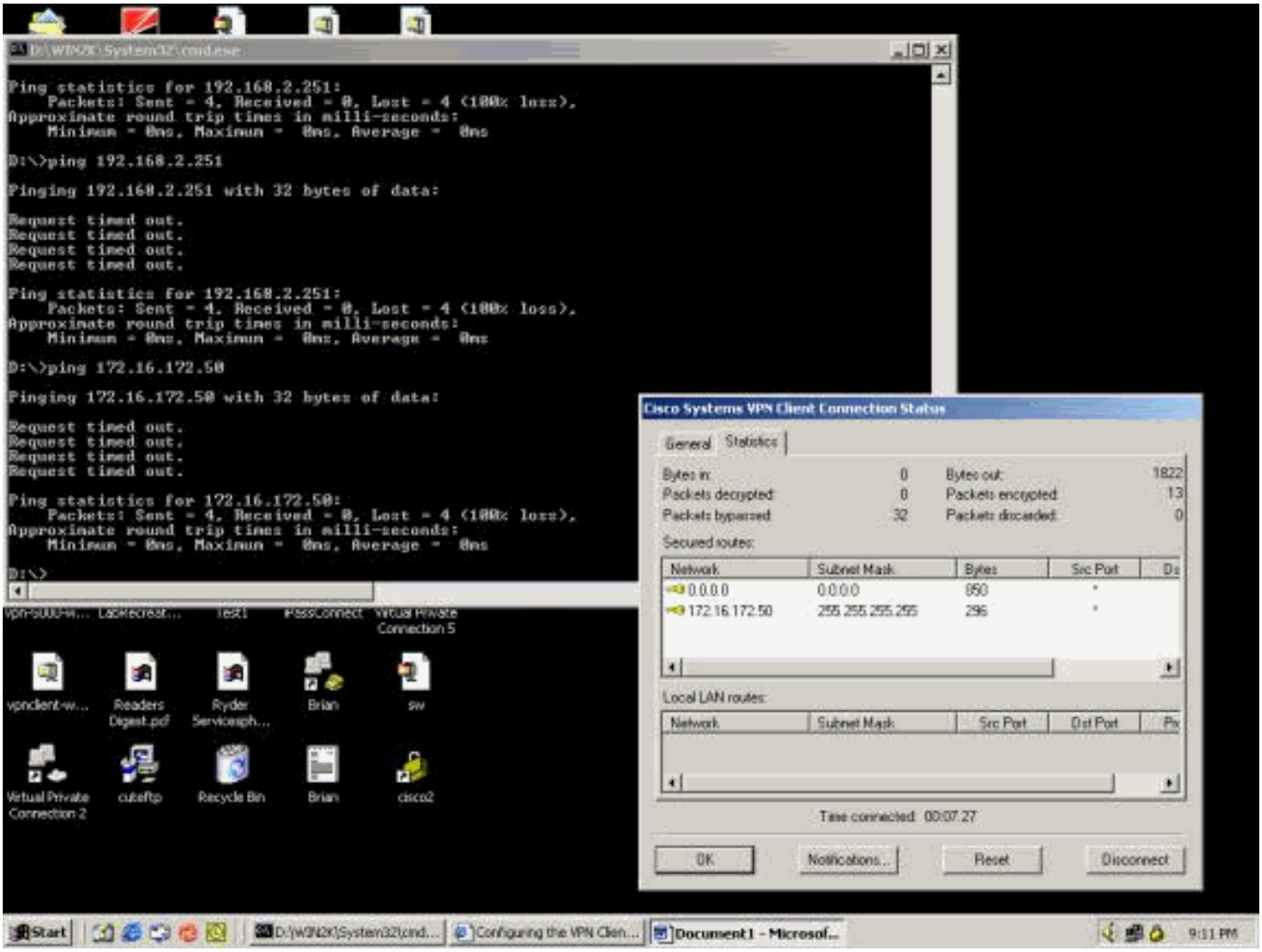
يوضح المثال التالي حالة لم يتم فيها فحص NAT-T على مركز التركيز. في العميل، تم التحقق من الاتصال النفقي الشفاف. وفي هذه الحالة، يتم إنشاء نفق IPSec بين العميل والمركز. ومع ذلك، فنظرا لفشل مفاوضات منفذ نفق IPSec، لم يتم تمرير أي بيانات بين العميل والمركز. على هذا النحو، تكون وحدات البايت التي يتم إرسالها واستقبالها صفر لجلسات عمل الوصول عن بعد.



يوضح المثال التالي إحصائيات عميل الشبكة الخاصة الظاهرية (VPN). لاحظ أن منفذ النفق الذي تم التفاوض عليه هو 0. هناك محاولة إختبار الاتصال 192.168.2.251 (الواجهة الخاصة لتركيز VPN 3000) و 172.16.172.50 من موجه الأمر DoS. ومع ذلك، تفشل هذه إختبارات الاتصال لأنه لم يتم التفاوض على أي منفذ نفق، وبالتالي، يتم تجاهل بيانات IPSec على خادم VPN البعيد.



يوضح المثال التالي أن عميل الشبكة الخاصة الظاهرية (VPN) يرسل بيانات مشفرة (13 حزمة). ولكن عدد الحزم التي تم فك تشفيرها هو صفر لخادم VPN البعيد، ولم يقم بإرسال أي بيانات مشفرة مرة أخرى. بما أنه لم يتم التفاوض على أي منفذ نفق، فإن خادم VPN البعيد يتجاهل الحزم ويرسل بيانات عدم الرد.



معلومات ذات صلة

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