配置多个 VPN 客户端到 Cisco VPN 3000 集中器的连接使用 NAT 穿越

目录

简介

本文显示如何在端口地址转换（PAT）/NAT设备后面的Cisco VPN客户端及远程Cisco VPN集中器之间配置网络地址转换穿越(NAT-T）。NAT-T可以在VPN客户端软件和VPN集中器之间，或者在NAT/PAT设备之后的集中器之间使用。当连接到运行Cisco IOS软件和PIX防火墙的Cisco路由器时，也可以使用NAT-T;不过，本文档中未介绍这些配置。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

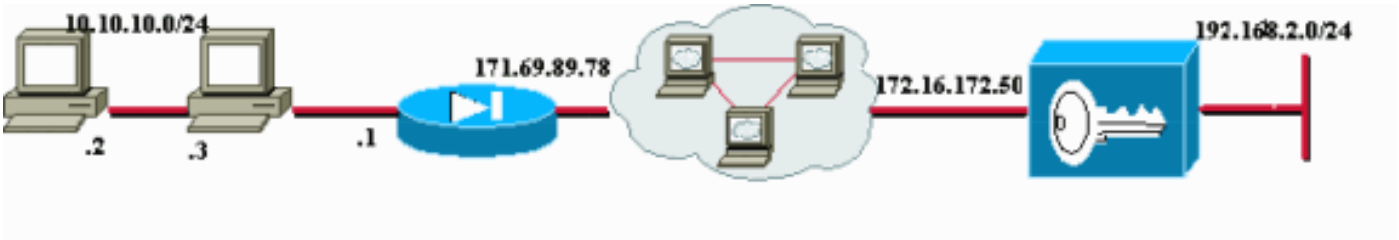
本文档中的信息基于以下软件和硬件版本：

- Cisco VPN 3000 集中器 4.0(1)B
- Cisco VPN 客户端：3.6.1 和 4.0(3) 版本
- Cisco PIX 防火墙（PAT 设备）版本 6.3(3)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

网络图

本文档使用以下网络设置：



在PIX防火墙之后的二个PC (10.10.10.2和10.10.10.3)上有VPN客户端软件。在本方案中，PIX只是简单地被用作PAT设备，并将这些地址PAT传输到171.69.89.78 。此处可以使用能够对多个内部连接执行 PAT 操作的任何设备。 VPN 3000 集中器的公共地址为 172.16.172.50。以下示例展示如何配置客户端和集中器，以便在IKE协商期间使用NAT-T。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

在NAT-T协商完成之后，发起人能使用任意随机的用户数据协议(UDP)端口(y)。目的端口必须是UDP4500 ，与UDP中的相同(Y， 4500 ），并且回应者也使用UDP (4500，Y)。后续的所有 Internet Key Exchange (IKE) 协商和重新生成密钥操作是在这些端口上完成的。在NAT-T协商期间，两个IPSec对等体与UDP端口协商，并且确定它们是否是在NAT/PAT设备之后。在NAT/PAT设备之后的IPSec对等体将IPSec-over-UDP NAT保活数据包发送到不在NAT/PAT设备之后的IPSec对等体。NAT-T使用端口4500，在UDP数据包封装IPSec信息数据流，从而为NAT设备提供端口信息。NAT-T 会自动检测所有 NAT 设备，并在必要时仅封装 IPSec 数据流。

在VPN 3000集中器实施 IPSec over NAT 转换时，IPSec over TCP 具有第一优先级，然后是NAT-T，最后是 IPSec over UDP。默认情况下，NAT-T 处于关闭状态。您需要使用位于 NAT Transparency的复选框启用NAT-T， NAT Transparency位于在隧道协议之下的IPSec配置之下。对于LAN-to-LAN隧道来说，您还必须在LAN-to-LAN配置IPSec NAT-T字段下启用NAT-T。

要使用 NAT-T，您必须完成以下步骤：

1. 在您已在 VPN 集中器前面配置的任何防火墙上打开端口 4500。
2. 使用端口 4500 将以前的 IPSec/UDP 配置项重新配置到其他端口。
3. 选择 **Configuration > Interfaces > Ethernet**，然后选择分段策略参数的第二个或第三个选项。这些选项允许数据流跨越整个NAT设备，此设备不支持IP分段;这些选项不会妨碍确实支持 IP 分段的 NAT 设备的操作。

配置 PIX

PIX 的相关配置输出如下所示：

PIX 防火墙

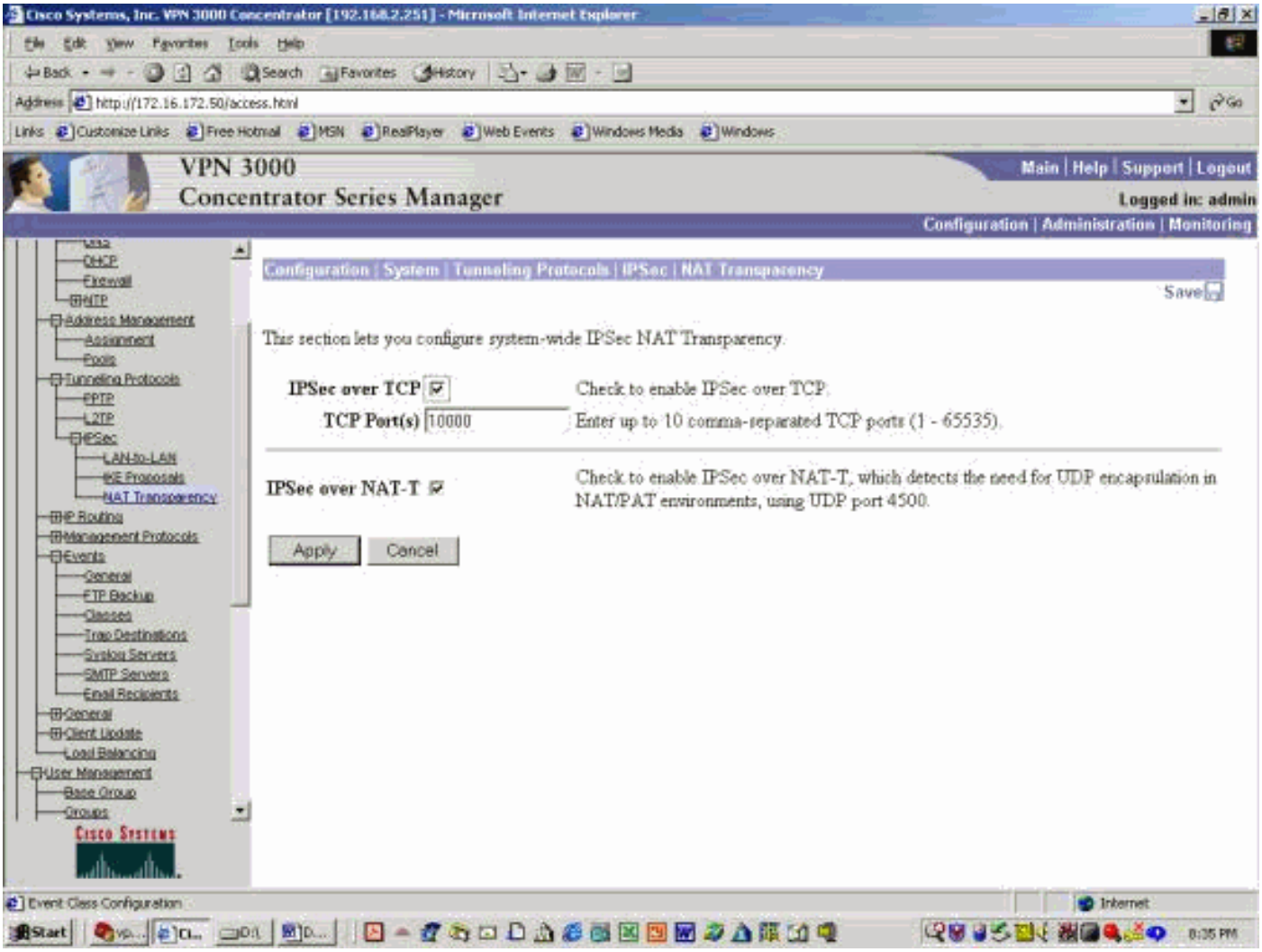
```
pix501(config)#
: Saved
:
PIX Version 6.3(3)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
ip address outside 171.69.89.78 255.255.254.0
ip address inside 10.10.10.1 255.255.255.0
...
global (outside) 1 interface nat (inside) 1 0.0.0.0
0.0.0.0 0 0 ... route outside 0.0.0.0 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]
```

配置VPN 3000集中器

本示例配置假设VPN 3000集中器已经配置来实现IP连通性，并且标准的(非NAT- T) VPN连接已经建立。

为了在早于4.1版本的VPN 3000集中器中启用NAT-T，请选择 **Configurations > System > Tunneling protocols > IPSec > NAT Transparency**，然后在集中器中检查NAT-T选项，如下例所示。默认情况下，NAT-T 选项处于关闭状态。

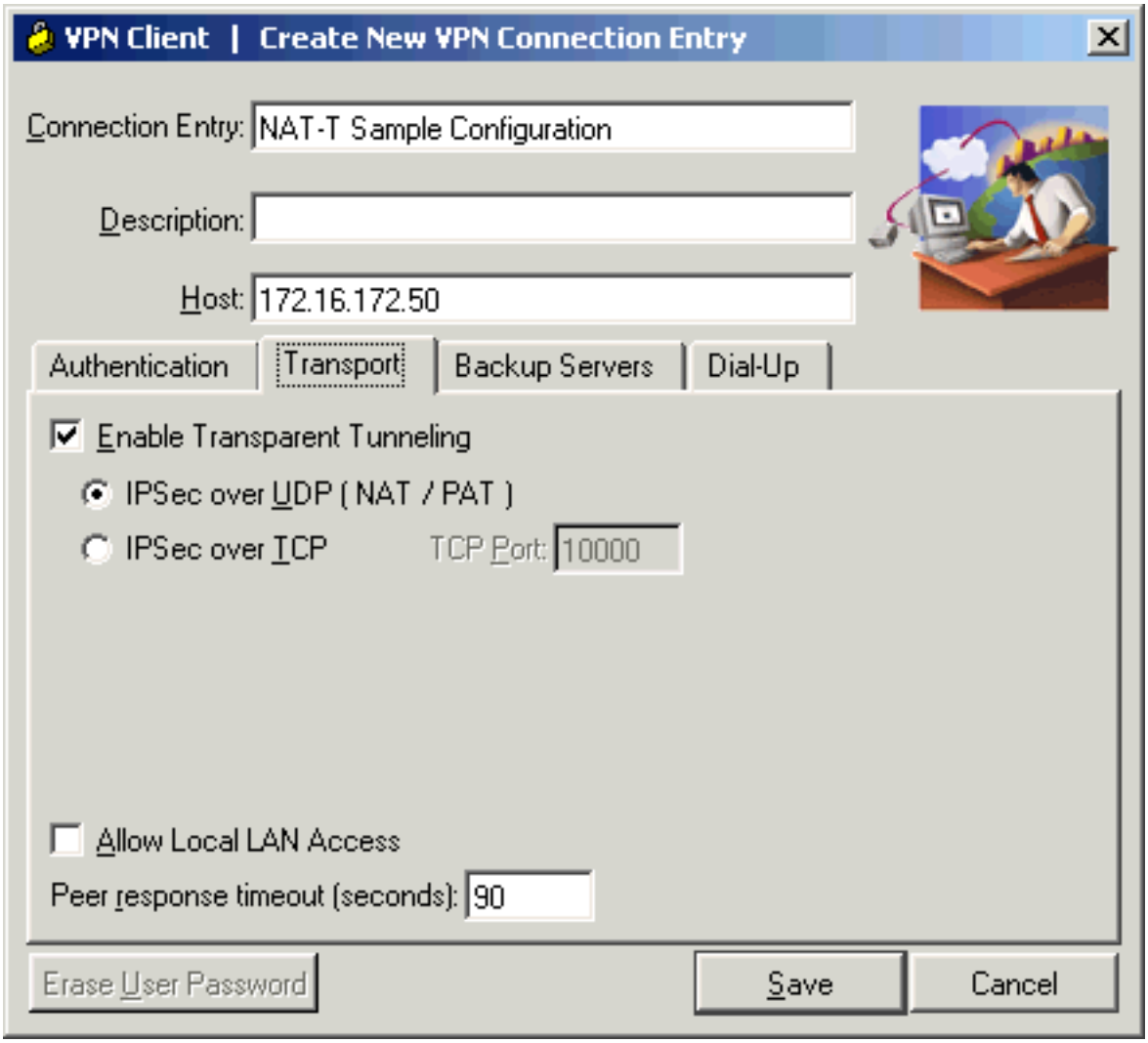
要启用VPN集中器4.1及以上版本的NAT-T，通过选择Configuration > Tunneling and Security > IPSec > NAT Transparency导向同一个NAT Transparency 窗口。



配置 VPN 客户端

要使用 NAT-T，请选中 **Enable Transparent Tunneling**。以下示例说明了 4.0 以后版本的 VPN 客户端中的此选项。

注意： VPN 客户端版本 3.x 中提供了同一配置选项。



验证

本部分所提供的信息可用于确认您的配置是否正常工作。

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

有关其他故障排除信息，请参阅 IP 安全故障排除 - 了解和使用 debug 命令。

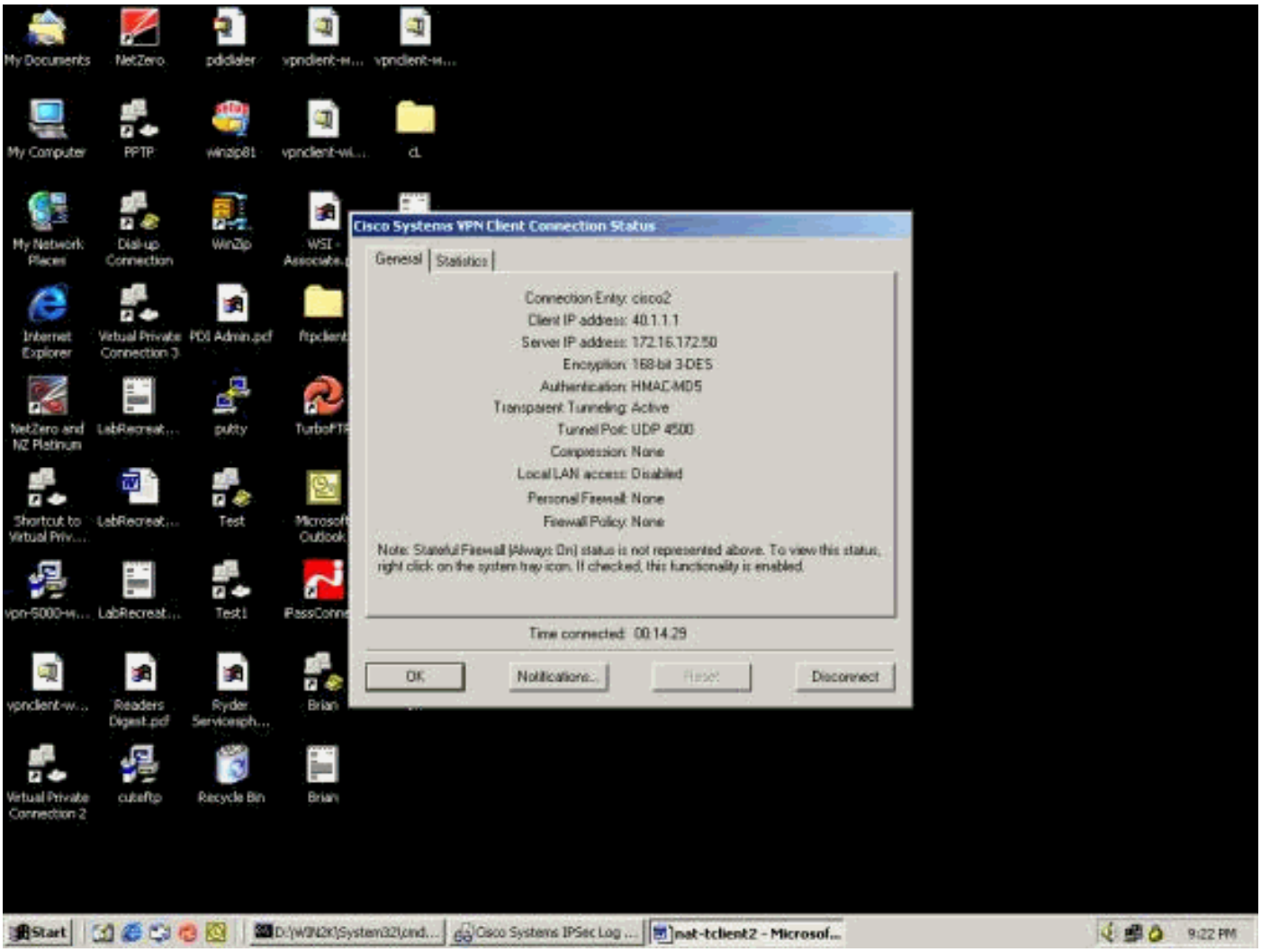
验证 PIX 配置

以下命令用于验证 PIX 配置：

- **show xlate** — 如下输出显示，PIX对二个VPN客户端软件使用不同的源端口，但目的地端口是相同。所有 IPSec 数据包是使用 UDP 端口 4500 包装的。后续的重新生成密钥协商也使用同样的源端口和目标端口。`pix501(config)# **show xlate** 3 in use, 4 most used 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** — 使用此命令显示地址解析协议(ARP)表，并确定是否ARP请求正在被处理。`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)#`

VPN 客户端统计信息

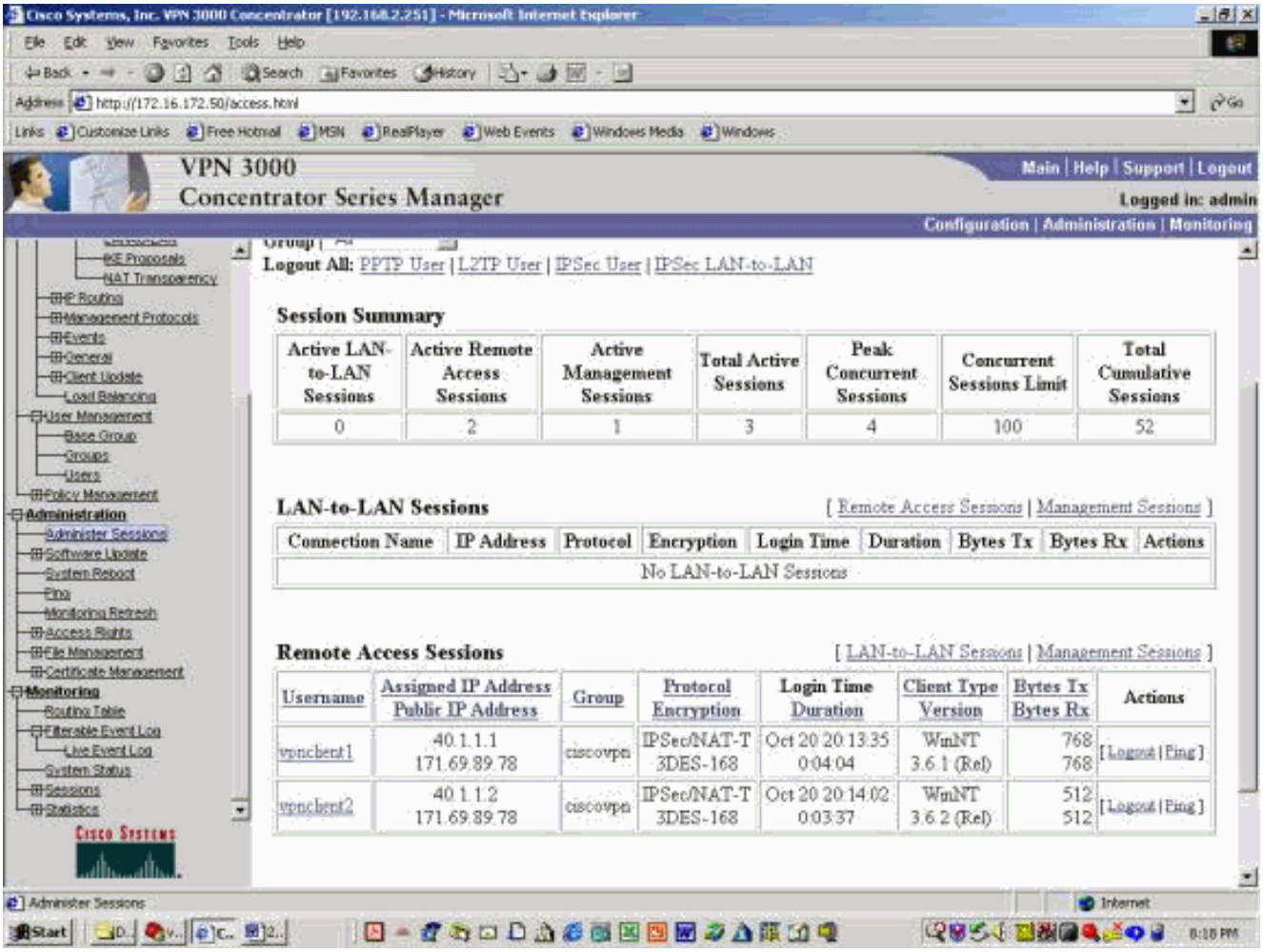
一旦设立VPN隧道，点击黄色锁定并选择**Status**。以下显示了一个类似窗口。注意隧道端口是UDP 4500，它证明您在使用NAT-T。



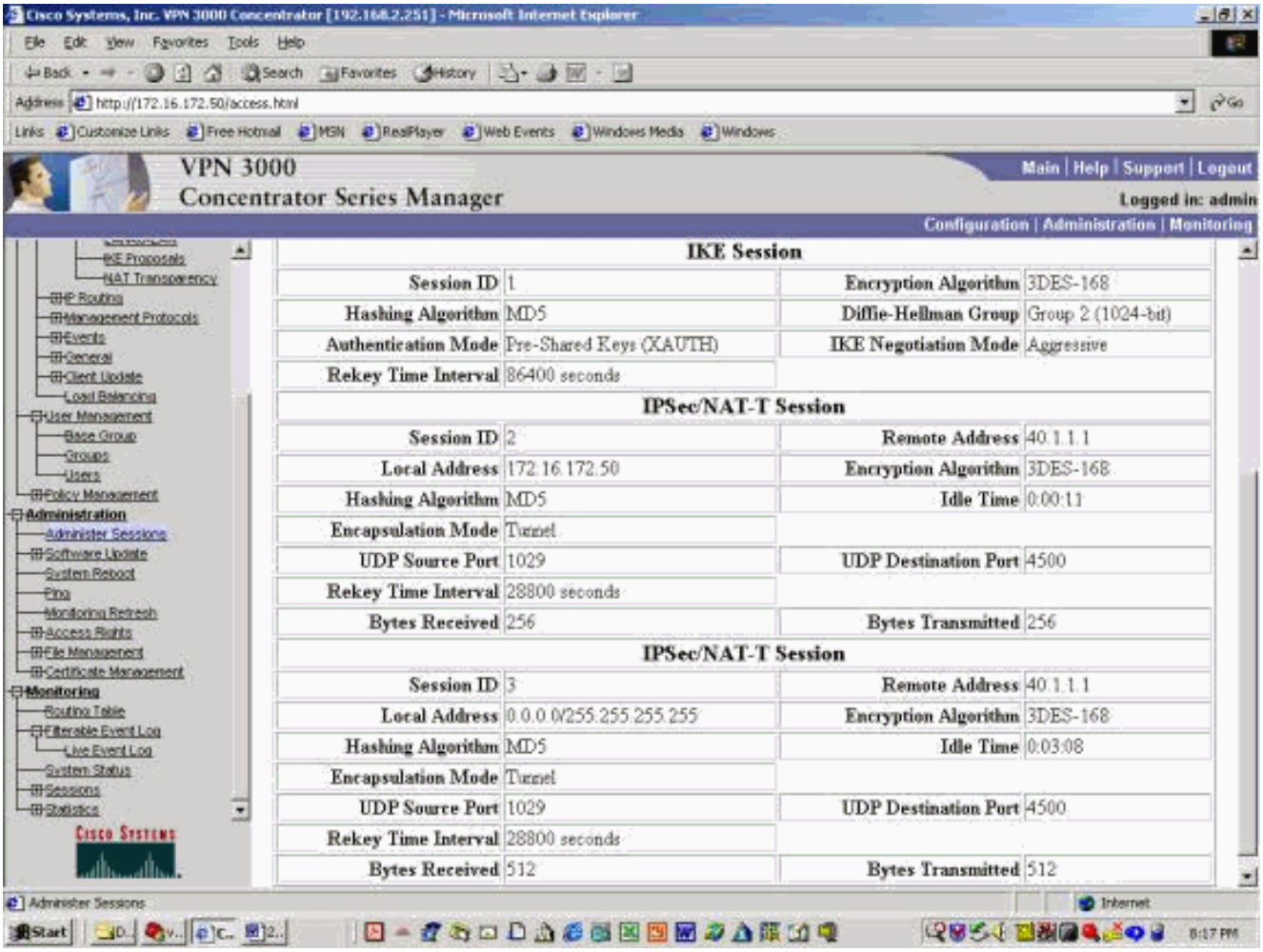
VPN 集中器统计数据

完成这些步骤：

1. 在 VPN 集中器上，选择 **Administration > Administrator Session**。可以在 Remote Access Sessions 下看到 VPN 客户端会话。以下示例显示二个客户端对VPN集中器设立了一个IPSec隧道之后的会话。这两个客户端都在使用公用 IP 地址 171.69.89.78，并且分别分配有 40.1.1.1 和 40.1.1.2。



2. 双击某个客户端用户名。此时将显示 IPSec/IKE 统计信息，如以下示例所示。客户端使用的UDP源端口是1029，目的地端口是4500。



故障排除

本部分提供的信息可用于对配置进行故障排除。

注意： 在发出 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

注意： 有关其他 PIX 故障排除信息，请参阅 IP 安全故障排除 - 了解和使用 debug 命令。

VPN 客户端日志

在已经安装VPN客户端软件的PC上，请在连接VPN集中器前打开Log Viewer。 以下日志输出突出显示了特定于 NAT-T 的消息：

```
1      21:06:48.208  10/18/02  Sev=Info/6   DIALER/0x63300002
Initiating connection.
2      21:06:48.218  10/18/02  Sev=Info/4   CM/0x63100002
Begin connection process
3      21:06:48.218  10/18/02  Sev=Info/4   CM/0x63100004
Establish secure connection using Ethernet
4      21:06:48.218  10/18/02  Sev=Info/4   CM/0x63100026
Attempt connection with server "172.16.172.50"
42     21:07:42.326  10/18/02  Sev=Info/6  IKE/0x6300003B
Attempting to establish a connection with 172.16.172.50.
43     21:07:42.366  10/18/02  Sev=Info/4  IKE/0x63000013
SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID, VID, VID)
 to 172.16.172.50
44     21:07:42.716  10/18/02  Sev=Info/5  IKE/0x6300002F
```

Received ISAKMP packet: peer = 172.16.172.50
45 21:07:42.716 10/18/02 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK AG (SA, KE, NON, ID, HASH, VID, VID, VID, VID, NAT-D, NAT-D, VID, VID) from 172.16.172.50 46 21:07:42.716 10/18/02 Sev=Info/5 IKE/0x63000059 Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100 47 21:07:42.716 10/18/02 Sev=Info/5 IKE/0x63000001 Peer is a Cisco-Unity compliant peer 48 21:07:42.716 10/18/02 Sev=Info/5 IKE/0x63000059 Vendor ID payload = 09002689DFD6B712 49 21:07:42.716 10/18/02 Sev=Info/5 IKE/0x63000001 **Peer supports XAUTH** 50 21:07:42.716 10/18/02 Sev=Info/5 IKE/0x63000059 Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100 51 21:07:42.716 10/18/02 Sev=Info/5 IKE/0x63000001 Peer supports DPD 52 21:07:42.716 10/18/02 Sev=Info/5 IKE/0x63000059 Vendor ID payload = 90CB80913EBB696E086381B5EC427B1F 53 21:07:42.716 10/18/02 Sev=Info/5 IKE/0x63000001 **Peer supports NAT-T** 54 21:07:42.716 10/18/02 Sev=Info/5 IKE/0x63000059 Vendor ID payload = 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000 55 21:07:42.716 10/18/02 Sev=Info/5 IKE/0x63000001 **Peer supports IKE fragmentation payloads** 56 21:07:42.716 10/18/02 Sev=Info/5 IKE/0x63000059 Vendor ID payload = 1F07F70EAA6514D3B0FA96542A500306 57 21:07:42.757 10/18/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT, NAT-D, NAT-D) to 172.16.172.50 58 21:07:42.767 10/18/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.16.172.50 59 21:07:42.767 10/18/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 172.16.172.50 60 21:07:42.767 10/18/02 Sev=Info/4 CM/0x63100015 **Launch xAuth application** 61 21:07:42.967 10/18/02 Sev=Info/4 IPSEC/0x63700014 Deleted all keys 62 21:07:59.801 10/18/02 Sev=Info/4 CM/0x63100017 xAuth application returned 63 21:07:59.801 10/18/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.16.172.50 64 21:08:00.101 10/18/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.16.172.50 65 21:08:00.101 10/18/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 172.16.172.50 66 21:08:00.101 10/18/02 Sev=Info/5 IKE/0x63000071 **Automatic NAT Detection Status: Remote end is NOT behind a NAT device This end IS behind a NAT device** 67 21:08:00.101 10/18/02 Sev=Info/4 CM/0x6310000E **Established Phase 1 SA. 1 Phase 1 SA in the system** 68 21:08:00.111 10/18/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.16.172.50 69 21:08:00.111 10/18/02 Sev=Info/5 IKE/0x6300005D Client sending a firewall request to concentrator 70 21:08:00.111 10/18/02 Sev=Info/5 IKE/0x6300005C Firewall Policy: Product=Cisco Integrated Client, Capability= (Centralized Protection Policy). 71 21:08:00.111 10/18/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.16.172.50 72 21:08:00.122 10/18/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.16.172.50 73 21:08:00.122 10/18/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 172.16.172.50 74 21:08:00.122 10/18/02 Sev=Info/5 IKE/0x63000010 MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: , value = 40.1.1.1 75 21:08:00.122 10/18/02 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value = 0x00000000 76 21:08:00.122 10/18/02 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_PFS: , value = 0x00000000 77 21:08:00.122 10/18/02 Sev=Info/5 IKE/0x6300000E 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 78 21:08:00.122 10/18/02 Sev=Info/5 IKE/0x6300000D **MODE_CFG_REPLY: Attribute = Recieved and using NAT-T port number , value = 0x00001194** 79 21:08:00.132 10/18/02 Sev=Info/4 CM/0x63100019 Mode Config data received 80 21:08:00.142 10/18/02 Sev=Info/5 IKE/0x63000055 Received a key request from Driver for IP address 172.16.172.50, GW IP = 172.16.172.50 81 21:08:00.142 10/18/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 172.16.172.50 82 21:08:00.142 10/18/02 Sev=Info/5 IKE/0x63000055 Received a key request from Driver for IP address 10.10.10.255, GW IP = 172.16.172.50 83 21:08:00.142 10/18/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 172.16.172.50 84 21:08:00.172 10/18/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.16.172.50 85 21:08:00.172 10/18/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:STATUS_RESP_LIFETIME) from 172.16.172.50 86 21:08:00.172 10/18/02 Sev=Info/5 IKE/0x63000044 RESPONDER-LIFETIME notify has value of 86400 seconds 87 21:08:00.172 10/18/02 Sev=Info/5 IKE/0x63000046 This SA has already been alive for 18 seconds, setting expiry to 86382 seconds from now 88 21:08:00.182 10/18/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.16.172.50 89 21:08:00.182 10/18/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME) from 172.16.172.50 90 21:08:00.182 10/18/02 Sev=Info/5 IKE/0x63000044 RESPONDER-LIFETIME notify has value of 28800 seconds 91 21:08:00.182 10/18/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK QM *(HASH) to 172.16.172.50 92 21:08:00.182 10/18/02 Sev=Info/5 IKE/0x63000058 **Loading IPsec SA (Message ID = 0x347A7363 OUTBOUND SPI = 0x02CC3526 INBOUND SPI = 0x5BEEBB4C)** 93 21:08:00.182 10/18/02 Sev=Info/5 IKE/0x63000025 **Loaded OUTBOUND ESP SPI: 0x02CC3526** 94 21:08:00.182 10/18/02 Sev=Info/5 IKE/0x63000026 **Loaded INBOUND ESP SPI: 0x5BEEBB4C** 95 21:08:00.182 10/18/02 Sev=Info/4 CM/0x6310001A **One secure connection established** 96 21:08:00.192 10/18/02 Sev=Info/6 DIALER/0x63300003 **Connection established.** 97 21:08:00.332 10/18/02 Sev=Info/5 IKE/0x6300002F

Received ISAKMP packet: peer = 172.16.172.50 98 21:08:00.332 10/18/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME) from 172.16.172.50 99 21:08:00.332 10/18/02 Sev=Info/5 IKE/0x63000044 RESPONDER-LIFETIME notify has value of 28800 seconds 100 21:08:00.332 10/18/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK QM *(HASH) to 172.16.172.50 101 21:08:00.342 10/18/02 Sev=Info/5 IKE/0x63000058 Loading IPsec SA (Message ID = 0x2F81FB2D OUTBOUND SPI = 0x3316C6C9 INBOUND SPI = 0x6B96ED76) 102 21:08:00.342 10/18/02 Sev=Info/5 IKE/0x63000025 **Loaded OUTBOUND ESP SPI: 0x3316C6C9** 103 21:08:00.342 10/18/02 Sev=Info/5 IKE/0x63000026 **Loaded INBOUND ESP SPI: 0x6B96ED76** 104 21:08:00.342 10/18/02 Sev=Info/4 CM/0x63100022 **Additional Phase 2 SA established.** 105 21:08:01.203 10/18/02 Sev=Info/4 IPSEC/0x63700014 Deleted all keys 106 21:08:01.203 10/18/02 Sev=Info/4 IPSEC/0x63700010 Created a new key structure 107 21:08:01.203 10/18/02 Sev=Info/4 IPSEC/0x6370000F Added key with SPI=0x2635cc02 into key list 108 21:08:01.203 10/18/02 Sev=Info/4 IPSEC/0x63700010 Created a new key structure 109 21:08:01.203 10/18/02 Sev=Info/4 IPSEC/0x6370000F Added key with SPI=0x4cbbee5b into key list 110 21:08:01.203 10/18/02 Sev=Info/4 IPSEC/0x63700010 Created a new key structure 111 21:08:01.203 10/18/02 Sev=Info/4 IPSEC/0x6370000F Added key with SPI=0xc9c61633 into key list 112 21:08:01.203 10/18/02 Sev=Info/4 IPSEC/0x63700010 Created a new key structure 113 21:08:01.203 10/18/02 Sev=Info/4 IPSEC/0x6370000F Added key with SPI=0x76ed966b into key list 114 21:08:10.216 10/18/02 Sev=Info/6 IKE/0x63000054 Sent a ping on the Public IPSec SA 115 21:08:20.381 10/18/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK INFO *(HASH, NOTIFY:HEARTBEAT) to 172.16.172.50 116 21:08:20.381 10/18/02 Sev=Info/6 IKE/0x63000052 Sent a ping on the IKE SA

VPN 集中器日志

如果要查看VPN集中器注册，请选择 **Monitoring > Filterable Event Log**，然后选择带有1-13个严格级别的事件类型 IKE, IKEDBG, IKEDECODE和IPSECDBG和IPSECDBG。

```
2835 10/20/2002 20:22:42.390 SEV=8 IKEDECODE/0 RPT=8190 171.69.89.78
  Exchange Type :Oakley Quick Mode
  Flags         :1   (ENCRYPT )
  Message ID    : 1b050792
  Length        : 52
 2838 10/20/2002 20:22:42.390 SEV=8 IKEDBG/0 RPT=9197 171.69.89.78
RECEIVED Message (msgid=1b050792) with payloads :
HDR + HASH (8) + NONE (0)
total length : 48
2840 10/20/2002 20:22:42.390 SEV=9 IKEDBG/0 RPT=9198 171.69.89.78
Group [ciscovpn] User [vpnclient2]
processing hash
2841 10/20/2002 20:22:42.390 SEV=9 IKEDBG/0 RPT=9199 171.69.89.78
Group [ciscovpn] User [vpnclient2]
loading all IPSEC SAs
 2842 10/20/2002 20:22:42.390 SEV=9 IKEDBG/1 RPT=793 171.69.89.78
Group [ciscovpn] User [vpnclient2]
Generating Quick Mode Key!
2843 10/20/2002 20:22:42.390 SEV=9 IKEDBG/1 RPT=794 171.69.89.78
Group [ciscovpn] User [vpnclient2]
Generating Quick Mode Key!
2844 10/20/2002 20:22:42.400 SEV=4 IKE/173 RPT=41 171.69.89.78
Group [ciscovpn] User [vpnclient2]
```

NAT-Traversal successfully negotiated! IPSec traffic will be encapsulated to pass through NAT devices. 2847 10/20/2002 20:22:42.400 SEV=7 IKEDBG/0 RPT=9200 171.69.89.78 Group [ciscovpn] User [vpnclient2] Loading host: Dst: 172.16.172.50 Src: 40.1.1.2 2849 10/20/2002 20:22:42.400 SEV=4 IKE/49 RPT=63 171.69.89.78 Group [ciscovpn] User [vpnclient2] Security negotiation complete for User (vpnclient2) Responder, Inbound SPI = 0x350f3cb1, Outbound SPI = 0xc74e30e5 2852 10/20/2002 20:22:42.400 SEV=9 IPSECDBG/6 RPT=309 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 2856 10/20/2002 20:22:42.400 SEV=9 IPSECDBG/1 RPT=1137 Processing KEY_ADD msg! 2857 10/20/2002 20:22:42.400 SEV=9 IPSECDBG/1 RPT=1138 key_msghdr2secassoc(): Enter 2858 10/20/2002 20:22:42.400 SEV=7 IPSECDBG/1 RPT=1139 No USER filter configured 2859 10/20/2002 20:22:42.400 SEV=9 IPSECDBG/1 RPT=1140 KeyProcessAdd: Enter 2860 10/20/2002 20:22:42.400 SEV=8 IPSECDBG/1 RPT=1141 KeyProcessAdd: Adding outbound SA 2861 10/20/2002 20:22:42.400 SEV=8 IPSECDBG/1 RPT=1142

KeyProcessAdd: src 172.16.172.50 mask 0.0.0.0, DST 40.1.1.2 mask 0.0.0.0 2862 10/20/2002 20:22:42.400 SEV=8 IPSECDBG/1 RPT=1143 KeyProcessAdd: FilterIpsecAddIkeSa success 2863 10/20/2002 20:22:42.400 SEV=9 IPSECDBG/6 RPT=310 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 2866 10/20/2002 20:22:42.400 SEV=9 IPSECDBG/1 RPT=1144 Processing KEY_UPDATE MSG! 2867 10/20/2002 20:22:42.400 SEV=9 IPSECDBG/1 RPT=1145 Update inbound SA addresses 2868 10/20/2002 20:22:42.400 SEV=9 IPSECDBG/1 RPT=1146 key_msghdr2secassoc(): Enter 2869 10/20/2002 20:22:42.400 SEV=7 IPSECDBG/1 RPT=1147 No USER filter configured 2870 10/20/2002 20:22:42.400 SEV=9 IPSECDBG/1 RPT=1148 KeyProcessUpdate: Enter 2871 10/20/2002 20:22:42.400 SEV=8 IPSECDBG/1 RPT=1149 KeyProcessUpdate: success 2872 10/20/2002 20:22:42.400 SEV=8 IKEDBG/7 RPT=63 IKE got a KEY_ADD MSG for SA: SPI = 0xc74e30e5 2873 10/20/2002 20:22:42.400 SEV=8 IKEDBG/0 RPT=9201 pitcher: rcv KEY_UPDATE, spi 0x350f3cb1 2874 10/20/2002 20:22:42.400 SEV=4 IKE/120 RPT=63 171.69.89.78 Group [ciscovpn] User [vpnclient2] PHASE 2 COMPLETED (msgid=1b050792) 2875 10/20/2002 20:22:42.430 SEV=8 IKEDECODE/0 RPT=8191 171.69.89.78 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 2882 10/20/2002 20:22:42.430 SEV=8 IKEDBG/0 RPT=9202 171.69.89.78 RECEIVED Message (msgid=cf9d1420) with payloads : HDR + HASH (8) + NONE (0) total length : 48 2884 10/20/2002 20:22:42.430 SEV=9 IKEDBG/0 RPT=9203 171.69.89.78 Group [ciscovpn] User [vpnclient2] processing hash 2885 10/20/2002 20:22:42.430 SEV=9 IKEDBG/0 RPT=9204 171.69.89.78 Group [ciscovpn] User [vpnclient2] loading all IPSEC SAs 2886 10/20/2002 20:22:42.430 SEV=9 IKEDBG/1 RPT=795 171.69.89.78 Group [ciscovpn] User [vpnclient2] Generating Quick Mode Key! 2887 10/20/2002 20:22:42.440 SEV=9 IKEDBG/1 RPT=796 171.69.89.78 Group [ciscovpn] User [vpnclient2] Generating Quick Mode Key! 2888 10/20/2002 20:22:42.440 SEV=4 IKE/173 RPT=42 171.69.89.78 **Group [ciscovpn] User [vpnclient2] NAT-Traversal successfully negotiated! IPSec traffic will be encapsulated to pass through NAT devices.** 2891 10/20/2002 20:22:42.440 SEV=7 IKEDBG/0 RPT=9205 171.69.89.78 Group [ciscovpn] User [vpnclient2] Loading subnet: DST: 0.0.0.0 mask: 0.0.0.0 Src: 40.1.1.2 2893 10/20/2002 20:22:42.440 SEV=4 IKE/49 RPT=64 171.69.89.78 Group [ciscovpn] User [vpnclient2] Security negotiation complete for User (vpnclient2) Responder, Inbound SPI = 0x2a2e2dcd, Outbound SPI = 0xf1f4d328 2896 10/20/2002 20:22:42.440 SEV=9 IPSECDBG/6 RPT=311 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 2900 10/20/2002 20:22:42.440 SEV=9 IPSECDBG/1 RPT=1150 Processing KEY_ADD MSG! 2901 10/20/2002 20:22:42.440 SEV=9 IPSECDBG/1 RPT=1151 key_msghdr2secassoc(): Enter 2902 10/20/2002 20:22:42.440 SEV=7 IPSECDBG/1 RPT=1152 No USER filter configured 2903 10/20/2002 20:22:42.440 SEV=9 IPSECDBG/1 RPT=1153 KeyProcessAdd: Enter 2904 10/20/2002 20:22:42.440 SEV=8 IPSECDBG/1 RPT=1154 KeyProcessAdd: Adding outbound SA 2905 10/20/2002 20:22:42.440 SEV=8 IPSECDBG/1 RPT=1155 KeyProcessAdd: src 0.0.0.0 mask 255.255.255.255, DST 40.1.1.2 mask 0.0.0.0 2906 10/20/2002 20:22:42.440 SEV=8 IPSECDBG/1 RPT=1156 KeyProcessAdd: FilterIpsecAddIkeSa success 2907 10/20/2002 20:22:42.440 SEV=9 IPSECDBG/6 RPT=312 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 2910 10/20/2002 20:22:42.440 SEV=9 IPSECDBG/1 RPT=1157 Processing KEY_UPDATE MSG! 2911 10/20/2002 20:22:42.440 SEV=9 IPSECDBG/1 RPT=1158 Update inbound SA addresses 2912 10/20/2002 20:22:42.440 SEV=9 IPSECDBG/1 RPT=1159 key_msghdr2secassoc(): Enter 2913 10/20/2002 20:22:42.440 SEV=7 IPSECDBG/1 RPT=1160 No USER filter configured 2914 10/20/2002 20:22:42.440 SEV=9 IPSECDBG/1 RPT=1161 KeyProcessUpdate: Enter 2915 10/20/2002 20:22:42.440 SEV=8 IPSECDBG/1 RPT=1162 KeyProcessUpdate: success 2916 10/20/2002 20:22:42.440 SEV=8 IKEDBG/7 RPT=64 IKE got a KEY_ADD MSG for SA: SPI = 0xf1f4d328 2917 10/20/2002 20:22:42.440 SEV=8 IKEDBG/0 RPT=9206 pitcher: rcv KEY_UPDATE, spi 0x2a2e2dcd 2918 10/20/2002 20:22:42.440 SEV=4 IKE/120 RPT=64 171.69.89.78 Group [ciscovpn] User [vpnclient2] PHASE 2 COMPLETED (msgid=cf9d1420) 2919 10/20/2002 20:22:44.680 SEV=7 IPSECDBG/1 RPT=1163 IPSec Inbound SA has received data! 2920 10/20/2002 20:22:44.680 SEV=8 IKEDBG/0 RPT=9207 pitcher: recv KEY_SA_ACTIVE spi 0x2a2e2dcd 2921 10/20/2002 20:22:44.680 SEV=8 IKEDBG/0 RPT=9208 KEY_SA_ACTIVE no old rekey centry found with new spi 0x2a2e2dcd, mess_id 0x0 2922 10/20/2002 20:22:47.530 SEV=9 IPSECDBG/18 RPT=828 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive packet: success 2923 10/20/2002 20:22:47.530 SEV=9 IPSECDBG/18 RPT=829 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive packet: success 2924 10/20/2002 20:22:48.280 SEV=9 IPSECDBG/17 RPT=668 Received an IPSEC-over-NAT-T NAT keepalive packet 2925 10/20/2002 20:22:52.390 SEV=9 IPSECDBG/17 RPT=669 **Received an IPSEC-over-NAT-T NAT keepalive packet** 2926 10/20/2002 20:22:52.720 SEV=7 IPSECDBG/1 RPT=1164 IPSec Inbound SA has received data! 2927 10/20/2002 20:22:52.720 SEV=8 IKEDBG/0 RPT=9209 pitcher: recv KEY_SA_ACTIVE spi 0x19fb2d12 2928 10/20/2002 20:22:52.720 SEV=8 IKEDBG/0 RPT=9210 KEY_SA_ACTIVE no old rekey centry found with new spi 0x19fb2d12, mess_id 0x0

2929 10/20/2002 20:22:56.530 SEV=9 IPSECDBG/18 RPT=830 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive packet: success 2930 10/20/2002 20:22:56.530 SEV=9 IPSECDBG/18 RPT=831 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive packet: success 2931 10/20/2002 20:22:58.300 SEV=8 IKEDECODE/0 RPT=8192 171.69.89.78 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 2938 10/20/2002 20:22:58.300 SEV=8 IKEDBG/0 RPT=9211 171.69.89.78 RECEIVED Message (msgid=d4a0ec25) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 76 2940 10/20/2002 20:22:58.300 SEV=9 IKEDBG/0 RPT=9212 171.69.89.78 Group [ciscovpn] User [vpnclient1] processing hash 2941 10/20/2002 20:22:58.300 SEV=9 IKEDBG/0 RPT=9213 171.69.89.78 Group [ciscovpn] User [vpnclient1] Processing Notify payload 2942 10/20/2002 20:22:58.300 SEV=8 IKEDECODE/0 RPT=8193 171.69.89.78 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 2948 10/20/2002 20:22:58.300 SEV=9 IKEDBG/41 RPT=336 171.69.89.78 Group [ciscovpn] User [vpnclient1] Received keep-alive of type Altiga keep-alive, not the negotiated type 2950 10/20/2002 20:22:58.310 SEV=8 IKEDECODE/0 RPT=8194 171.69.89.78 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 2957 10/20/2002 20:22:58.310 SEV=8 IKEDBG/0 RPT=9214 171.69.89.78 RECEIVED Message (msgid=d196c721) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 80 2959 10/20/2002 20:22:58.310 SEV=9 IKEDBG/0 RPT=9215 171.69.89.78 Group [ciscovpn] User [vpnclient1] processing hash 2960 10/20/2002 20:22:58.310 SEV=9 IKEDBG/0 RPT=9216 171.69.89.78 Group [ciscovpn] User [vpnclient1] Processing Notify payload 2961 10/20/2002 20:22:58.310 SEV=8 IKEDECODE/0 RPT=8195 171.69.89.78 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 2967 10/20/2002 20:22:58.310 SEV=9 IKEDBG/36 RPT=92 171.69.89.78 Group [ciscovpn] User [vpnclient1] Sending keep-alive of type DPD R-U-THERE-ACK (seq number 0x2d932552) 2969 10/20/2002 20:22:58.310 SEV=9 IKEDBG/0 RPT=9217 171.69.89.78 Group [ciscovpn] User [vpnclient1] constructing blank hash 2970 10/20/2002 20:22:58.310 SEV=9 IKEDBG/0 RPT=9218 171.69.89.78 Group [ciscovpn] User [vpnclient1] constructing qm hash 2971 10/20/2002 20:22:58.310 SEV=8 IKEDBG/0 RPT=9219 171.69.89.78 SENDING Message (msgid=d678099) with payloads : HDR + HASH (8) + NOTIFY (11) total length : 80 2973 10/20/2002 20:23:02.400 SEV=8 IKEDECODE/0 RPT=8196 171.69.89.78 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 2980 10/20/2002 20:23:02.400 SEV=8 IKEDBG/0 RPT=9220 171.69.89.78 RECEIVED Message (msgid=317b646a) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 76 2982 10/20/2002 20:23:02.400 SEV=9 IKEDBG/0 RPT=9221 171.69.89.78 Group [ciscovpn] User [vpnclient2] processing hash 2983 10/20/2002 20:23:02.400 SEV=9 IKEDBG/0 RPT=9222 171.69.89.78 Group [ciscovpn] User [vpnclient2] Processing Notify payload 2984 10/20/2002 20:23:02.400 SEV=8 IKEDECODE/0 RPT=8197 171.69.89.78 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 2990 10/20/2002 20:23:02.400 SEV=9 IKEDBG/41 RPT=337 171.69.89.78 Group [ciscovpn] User [vpnclient2] Received keep-alive of type Altiga keep-alive, not the negotiated type 2992 10/20/2002 20:23:02.410 SEV=9 IPSECDBG/17 RPT=670 Received an IPSEC-over-NAT-T NAT keepalive packet 2993 10/20/2002 20:23:05.530 SEV=9 IPSECDBG/18 RPT=832 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive packet: success 2994 10/20/2002 20:23:05.530 SEV=9 IPSECDBG/18 RPT=833 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive packet: success 2995 10/20/2002 20:23:08.310 SEV=9 IPSECDBG/17 RPT=671 Received an IPSEC-over-NAT-T NAT keepalive packet 2996 10/20/2002 20:23:12.420 SEV=9 IPSECDBG/17 RPT=672 Received an IPSEC-over-NAT-T NAT keepalive packet 2997 10/20/2002 20:23:14.530 SEV=9 IPSECDBG/18 RPT=834 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive packet: success 2998 10/20/2002 20:23:14.530 SEV=9 IPSECDBG/18 RPT=835 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive packet: success 2999 10/20/2002 20:23:18.330 SEV=8 IKEDECODE/0 RPT=8198 171.69.89.78 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 3006 10/20/2002 20:23:18.330 SEV=8 IKEDBG/0 RPT=9223 171.69.89.78 RECEIVED Message (msgid=f6457474) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 76 3008 10/20/2002 20:23:18.330 SEV=9 IKEDBG/0 RPT=9224 171.69.89.78 Group [ciscovpn] User [vpnclient1] processing hash 3009 10/20/2002 20:23:18.330 SEV=9 IKEDBG/0 RPT=9225 171.69.89.78 Group [ciscovpn] User [vpnclient1] Processing Notify payload 3010 10/20/2002 20:23:18.330 SEV=8 IKEDECODE/0 RPT=8199 171.69.89.78 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 3016 10/20/2002 20:23:18.330 SEV=9 IKEDBG/41 RPT=338 171.69.89.78 Group [ciscovpn] User [vpnclient1] Received keep-alive of type Altiga keep-alive, not the negotiated type 3018

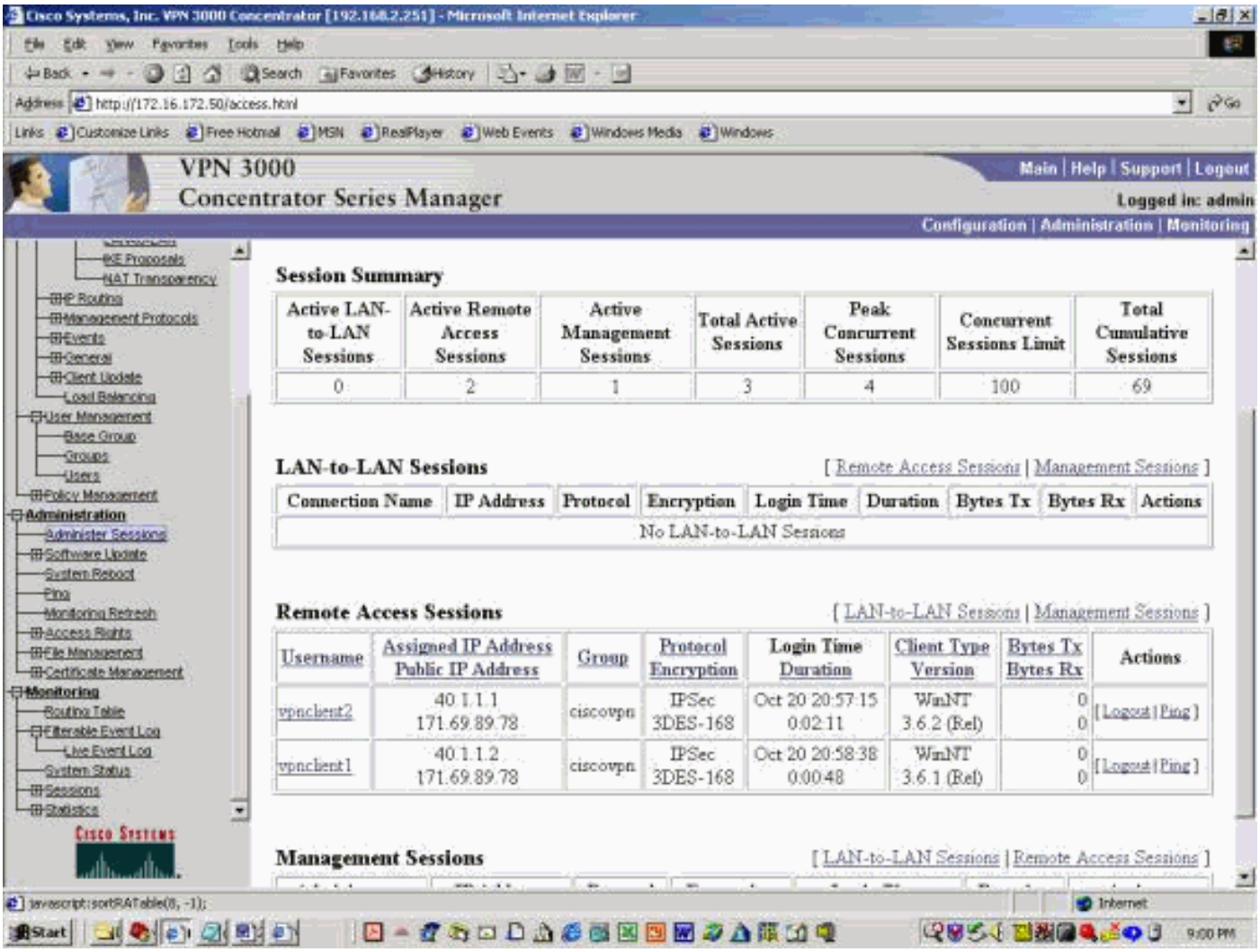
10/20/2002 20:23:18.330 SEV=9 IPSECDBG/17 RPT=673 Received an IPSEC-over-NAT-T NAT keepalive packet 3019 10/20/2002 20:23:22.430 SEV=8 IKEDECODE/0 RPT=8200 171.69.89.78 ISAKMP HEADER : (Version 1.0) Initiator Cookie(8): C5 A0 F0 8B 69 60 D7 47 Responder Cookie(8): 48 65 B1 6F 36 1F 9D 3A Next Payload : HASH (8) Exchange Type : Oakley Informational Flags : 1 (ENCRYPT) Message ID : 358ae39e Length : 76 3026 10/20/2002 20:23:22.430 SEV=8 IKEDBG/0 RPT=9226 171.69.89.78 RECEIVED Message (msgid=358ae39e) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 76 3028 10/20/2002 20:23:22.430 SEV=9 IKEDBG/0 RPT=9227 171.69.89.78 Group [ciscovpn] User [vpnclient2] processing hash 3029 10/20/2002 20:23:22.430 SEV=9 IKEDBG/0 RPT=9228 171.69.89.78 Group [ciscovpn] User [vpnclient2] Processing Notify payload 3030 10/20/2002 20:23:22.430 SEV=8 IKEDECODE/0 RPT=8201 171.69.89.78 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 3036 10/20/2002 20:23:22.430 SEV=9 IKEDBG/41 RPT=339 171.69.89.78 Group [ciscovpn] User [vpnclient2] Received keep-alive of type Altiga keep-alive, not the negotiated type 3038 10/20/2002 20:23:22.430 SEV=9 IPSECDBG/17 RPT=674 Received an IPSEC-over-NAT-T NAT keepalive packet 3039 10/20/2002 20:23:23.530 SEV=9 IPSECDBG/18 RPT=836 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive packet: success 3040 10/20/2002 20:23:23.530 SEV=9 IPSECDBG/18 RPT=837 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive packet: success 3041 10/20/2002 20:23:28.340 SEV=9 IPSECDBG/17 RPT=675 Received an IPSEC-over-NAT-T NAT keepalive packet 3042 10/20/2002 20:23:32.440 SEV=9 IPSECDBG/17 RPT=676 Received an IPSEC-over-NAT-T NAT keepalive packet 3043 10/20/2002 20:23:32.530 SEV=9 IPSECDBG/18 RPT=838 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive packet: success 3044 10/20/2002 20:23:32.530 SEV=9 IPSECDBG/18 RPT=839 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive packet: success 3045 10/20/2002 20:23:38.360 SEV=8 IKEDECODE/0 RPT=8202 171.69.89.78 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 3052 10/20/2002 20:23:38.360 SEV=8 IKEDBG/0 RPT=9229 171.69.89.78 RECEIVED Message (msgid=fa8597e6) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 76 3054 10/20/2002 20:23:38.360 SEV=9 IKEDBG/0 RPT=9230 171.69.89.78 Group [ciscovpn] User [vpnclient1] processing hash 3055 10/20/2002 20:23:38.360 SEV=9 IKEDBG/0 RPT=9231 171.69.89.78 Group [ciscovpn] User [vpnclient1] Processing Notify payload 3056 10/20/2002 20:23:38.360 SEV=8 IKEDECODE/0 RPT=8203 171.69.89.78 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 3062 10/20/2002 20:23:38.360 SEV=9 IKEDBG/41 RPT=340 171.69.89.78 Group [ciscovpn] User [vpnclient1] Received keep-alive of type Altiga keep-alive, not the negotiated type 3064 10/20/2002 20:23:38.360 SEV=9 IPSECDBG/17 RPT=677 Received an IPSEC-over-NAT-T NAT keepalive packet 3065 10/20/2002 20:23:41.530 SEV=9 IPSECDBG/18 RPT=840 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive packet: success 3066 10/20/2002 20:23:41.530 SEV=9 IPSECDBG/18 RPT=841 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive packet: success 3067 10/20/2002 20:23:42.470 SEV=8 IKEDECODE/0 RPT=8204 171.69.89.78 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) 3073 10/20/2002 20:23:42.470 SEV=8 IKEDECODE/0 RPT=8204 171.69.89.78 Message ID : c892dd4c Length : 76 RECEIVED Message (msgid=c892dd4c) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 76 3076 10/20/2002 20:23:42.470 SEV=9 IKEDBG/0 RPT=9233 171.69.89.78 Group [ciscovpn] User [vpnclient2] processing hash 3077 10/20/2002 20:23:42.470 SEV=9 IKEDBG/0 RPT=9234 171.69.89.78 Group [ciscovpn] User [vpnclient2] Processing Notify payload 3078 10/20/2002 20:23:42.470 SEV=8 IKEDECODE/0 RPT=8205 171.69.89.78 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 3084 10/20/2002 20:23:42.470 SEV=9 IKEDBG/41 RPT=341 171.69.89.78 Group [ciscovpn] User [vpnclient2] Received keep-alive of type Altiga keep-alive, not the negotiated type 3086 10/20/2002 20:23:42.470 SEV=9 IPSECDBG/17 RPT=678 Received an IPSEC-over-NAT-T NAT keepalive packet 3087 10/20/2002 20:23:48.370 SEV=9 IPSECDBG/17 RPT=679 Received an IPSEC-over-NAT-T NAT keepalive packet 3088 10/20/2002 20:23:50.530 SEV=9 IPSECDBG/18 RPT=842 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive packet: success 3089 10/20/2002 20:23:50.530 SEV=9 IPSECDBG/18 RPT=843 171.69.89.78 Xmit IPSEC-over-UDP NAT keepalive packet: success 3090 10/20/2002 20:23:52.470 SEV=9 IPSECDBG/17 RPT=680 Received an IPSEC-over-NAT-T NAT keepalive packet 3091 10/20/2002 20:23:58.380 SEV=8 IKEDECODE/0 RPT=8206 171.69.89.78 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 3098 10/20/2002 20:23:58.390 SEV=8 IKEDBG/0 RPT=9235 171.69.89.78 RECEIVED Message (msgid=943c7d99) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 76 3100 10/20/2002 20:23:58.390 SEV=9 IKEDBG/0 RPT=9236 171.69.89.78 Group [ciscovpn] User [vpnclient1] processing hash 3101 10/20/2002 20:23:58.390 SEV=9 IKEDBG/0 RPT=9237 171.69.89.78 Group [ciscovpn] User [vpnclient1] Processing Notify payload 3102 10/20/2002 20:23:58.390 SEV=8 IKEDECODE/0 RPT=8207

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

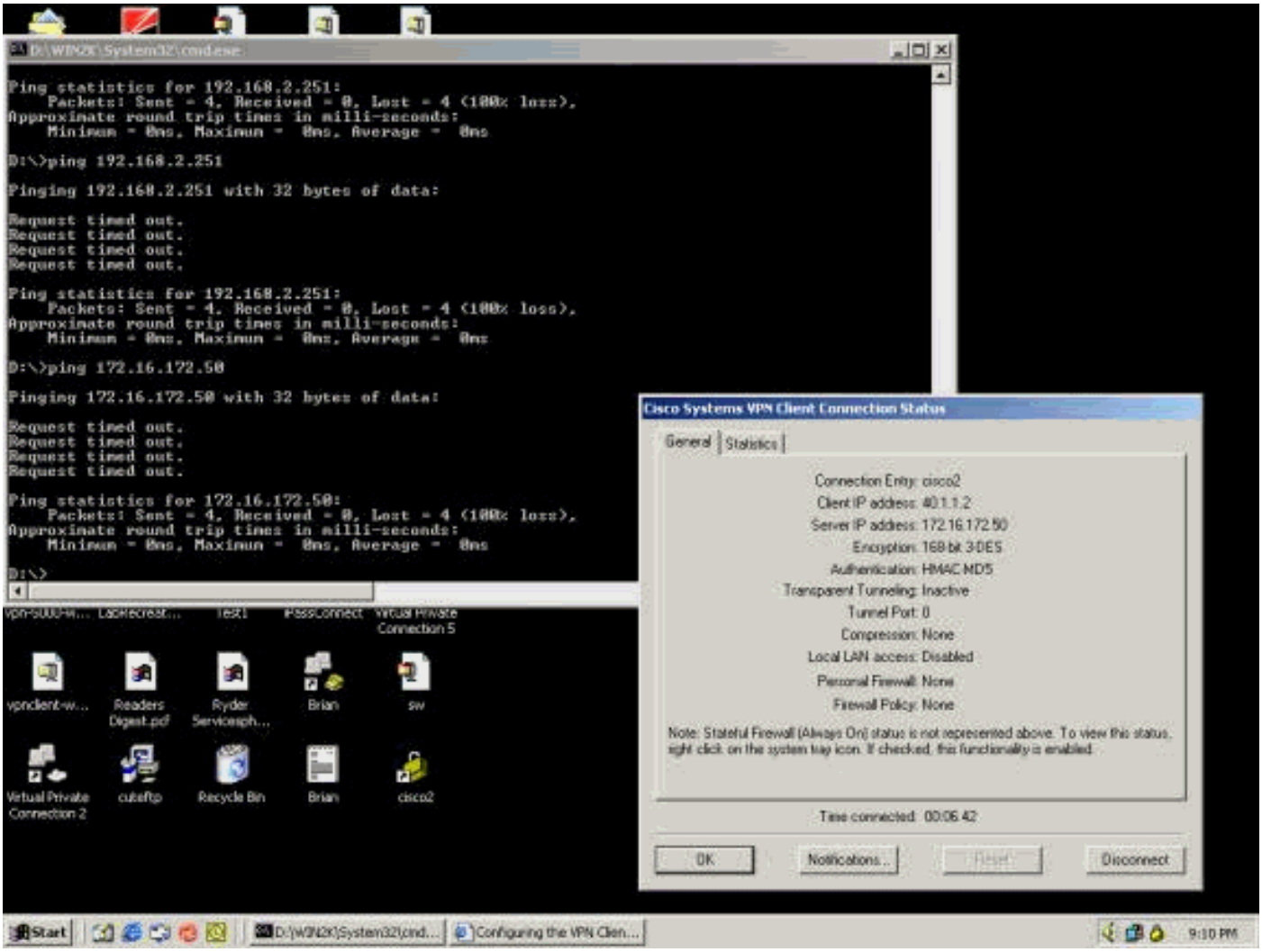
其他故障排除

NAT-T 使用端口 4500 将 IPSec 数据流封装在 UDP 数据报中。如果NAT-T不是在VPN集中器上被检查的，或NAT 透明度不是在VPN客户端被软件检查的，则IPSec隧道设立。然而，您不能传递任何数据。开始操作让NAT-T时，您必须在集中器上检查NAT，同时在路由器上对NAT 透明度进行检查 (通过UDP)。

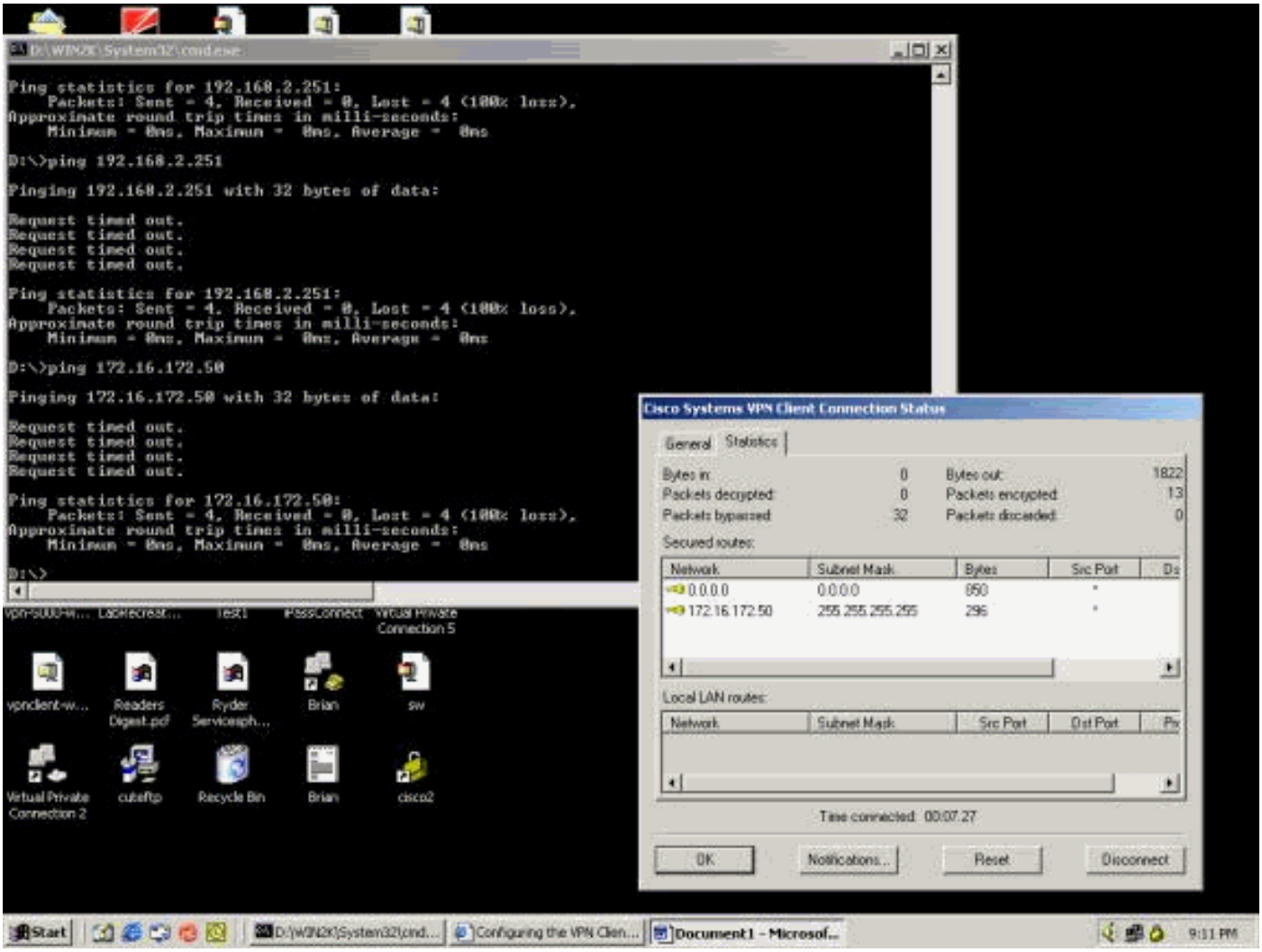
下面的示例显示NAT-T未在集中器中查看的一种情况。在客户端上，已选中 Transparent Tunneling。在这种情况下，将在客户端和集中器之间建立 IPSec 隧道。然而，由于IPSec隧道端口协商失败，客户端和集中器之间没有数据通过。这样，远程访问会话的传送和接收字节数为零。



以下示例显示了 VPN 客户端的统计信息。请注意，协商的隧道端口为 0。通过DOS命令，尝试ping 192.168.2.251 (VPN 3000集中器的专用接口)和172.16.172.50。然而，这些ping的失败原因是隧道端口没有协商，因此，IPSec数据在远程VPN服务器上被丢弃。



以下示例显示 VPN 客户端正在发送加密数据（13 个数据包）。但为远程VPN服务器的解密的数据包的数量是零，并且还未送回任何加密数据。因为隧道端口未协商，所以远程VPN服务器丢弃信息包并且发送不回复的数据。



相关信息

- Cisco VPN 3000 系列集中器支持页
- Cisco VPN 3000 系列客户端支持页
- IPSec 支持页面
- 技术支持和文档 - Cisco Systems