NAT-Traversal을 사용하여 Cisco VPN 3000 Concentrator에 여러 VPN 클라이언트 구성

목차

소개

이 문서에서는 PAT(Port Address Translation)/NAT 디바이스 및 원격 Cisco VPN Concentrator 뒤에 있는 Cisco VPN 클라이언트 간에 NAT-T(Network Address Translation Traversal)를 구성하는 방법을 보여 줍니다. NAT-T는 VPN 클라이언트와 VPN Concentrator 간 또는 NAT/PAT 디바이스 뒤에 있는 Concentrator 간에 사용할 수 있습니다. NAT-T는 Cisco IOS® 소프트웨어 및 PIX Firewall을 실행하는 Cisco 라우터에 연결할 때도 사용할 수 있습니다. 그러나 이 문서에서는 이러한 구성에 대해 다루지 않습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco VPN 3000 Concentrator 4.0(1)B
- Cisco VPN 클라이언트: 3.6.1 및 4.0(3) Rel
- Cisco PAT(PAT Firewall) 버전 6.3(3)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.

PIX 방화벽 뒤에 두 PC(10.10.10.2 및 10.10.10.3)에 VPN 클라이언트가 있습니다. 이 시나리오의 PAT는 단순히 PAT 장치로 사용되고 이 주소에서 PAT를 171.69.89.78으로 수행합니다. 여기서 여러 내부 연결을 PAT할 수 있는 모든 장치를 사용할 수 있습니다. VPN 3000 Concentrator 공용 주소는 172.16.172.50입니다. 다음 예는 IKE 협상 중에 NAT-T가 사용하도록 클라이언트 및 Concentrator를 구성하는 방법을 보여줍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

배경 정보

NAT-T 협상이 완료되면 개시자는 임의의 UDP(User Datagram Protocol) 포트(Y)를 사용할 수 있습니다. 대상 포트는 UDP(Y, 4500)와 마찬가지로 UDP 4500이어야 하며, 응답자는 UDP(4500, Y)를 사용합니다. 모든 후속 IKE(Internet Key Exchange) 협상 및 재키는 이러한 포트에서 수행됩니다. NAT-T 협상 중에 IPSec 피어가 UDP 포트를 협상하고 NAT/PAT 디바이스 뒤에 있는지 확인합니다. NAT/PAT 디바이스 뒤에 있는 IPSec 피어는 IPSec-over-UDP NAT keepalive 패킷을 NAT/PAT 디바이스 뒤에 없는 IPSec 피어로 전송합니다. NAT-T는 포트 4500을 사용하여 UDP 데이터그램에서 IPSec 트래픽을 캡슐화하여 NAT 디바이스에 포트 정보를 제공합니다. NAT-T는 모든 NAT 디바이스를 자동으로 탐지하고 필요한 경우 IPSec 트래픽만 캡슐화합니다.

VPN 3000 Concentrator에서 IPSec over NAT 변환을 구현할 경우, TCP를 통한 IPSec이 우선하며, NAT-T, IPSec over UDP가 우선합니다. 기본적으로 NAT-T는 꺼져 있습니다. NAT Transparency(NAT 투명도)에 있는 Tunneling Protocols(터널링 프로토콜) 아래의 IPSec 컨피그레이션 확인란을 사용하여 NAT-T를 활성화해야 합니다. 또한 LAN-to-LAN 터널의 경우 LAN-to-LAN 컨피그레이션 IPSec NAT-T 필드에서 NAT-T를 켜야 합니다.

NAT-T를 사용하려면 다음 단계를 완료해야 합니다.

1. VPN Concentrator 앞에 구성한 모든 방화벽에서 포트 4500을 엽니다.

2. 포트 4500을 사용하여 이전 IPSec/UDP 구성을 다른 포트로 재구성합니다.
3. Configuration **> Interfaces > Ethernet**을 선택하고 Fragmentation Policy 매개변수에 대한 두 번째 또는 세 번째 옵션을 선택합니다.이러한 옵션을 사용하면 트래픽이 IP 단편화를 지원하지 않는 NAT 디바이스를 통해 이동할 수 있습니다. IP 프래그먼트화를 지원하는 NAT 디바이스의 작동을 방해하지 않습니다.

PIX 구성

PIX에 대한 관련 컨피그레이션 출력은 다음과 같습니다.

PIX 방화벽

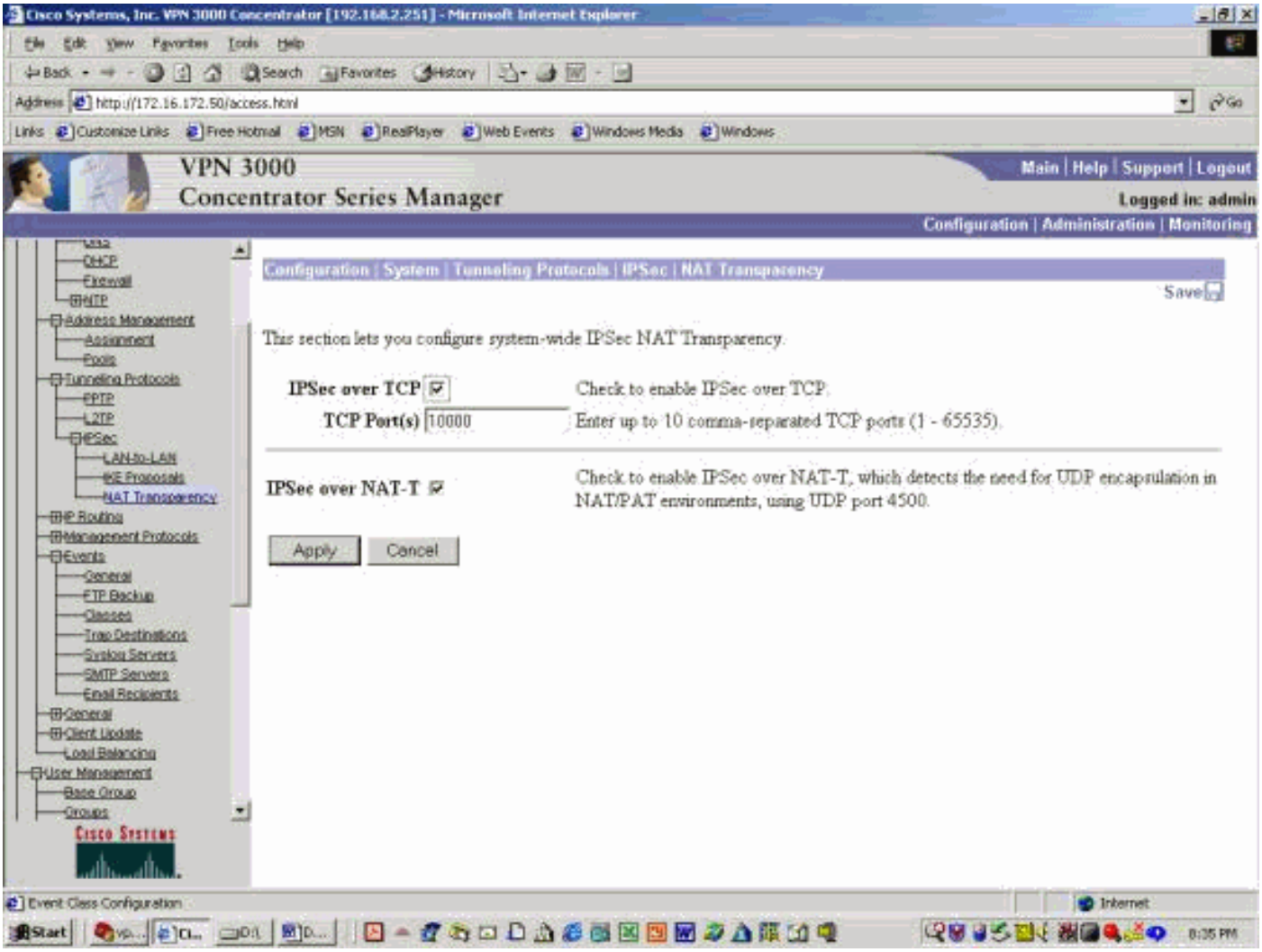
```
pix501(config)#
: Saved
:
PIX Version 6.3(3)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
ip address outside 171.69.89.78 255.255.254.0
ip address inside 10.10.10.1 255.255.255.0
...
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
...
route outside 0.0.0.0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

VPN 3000 Concentrator 구성

이 샘플 컨피그레이션에서는 VPN 3000 Concentrator가 IP 연결용으로 이미 구성되어 있고 표준(비 NAT-T) VPN 연결이 이미 설정되어 있다고 가정합니다.

버전 4.1 이전 VPN 3000 Concentrator 릴리스에서 NAT-T를 활성화하려면 Configurations(구성) **> System(시스템) > Tunneling protocols(터널링 프로토콜) > IPSec > NAT Transparency(NAT 투명도)를 선택한** 다음 아래 예와 같이 Concentrator에서 **IPSEC OVER NAT-T** 옵션을 선택합니다. NAT-T 옵션은 기본적으로 꺼져 있습니다.

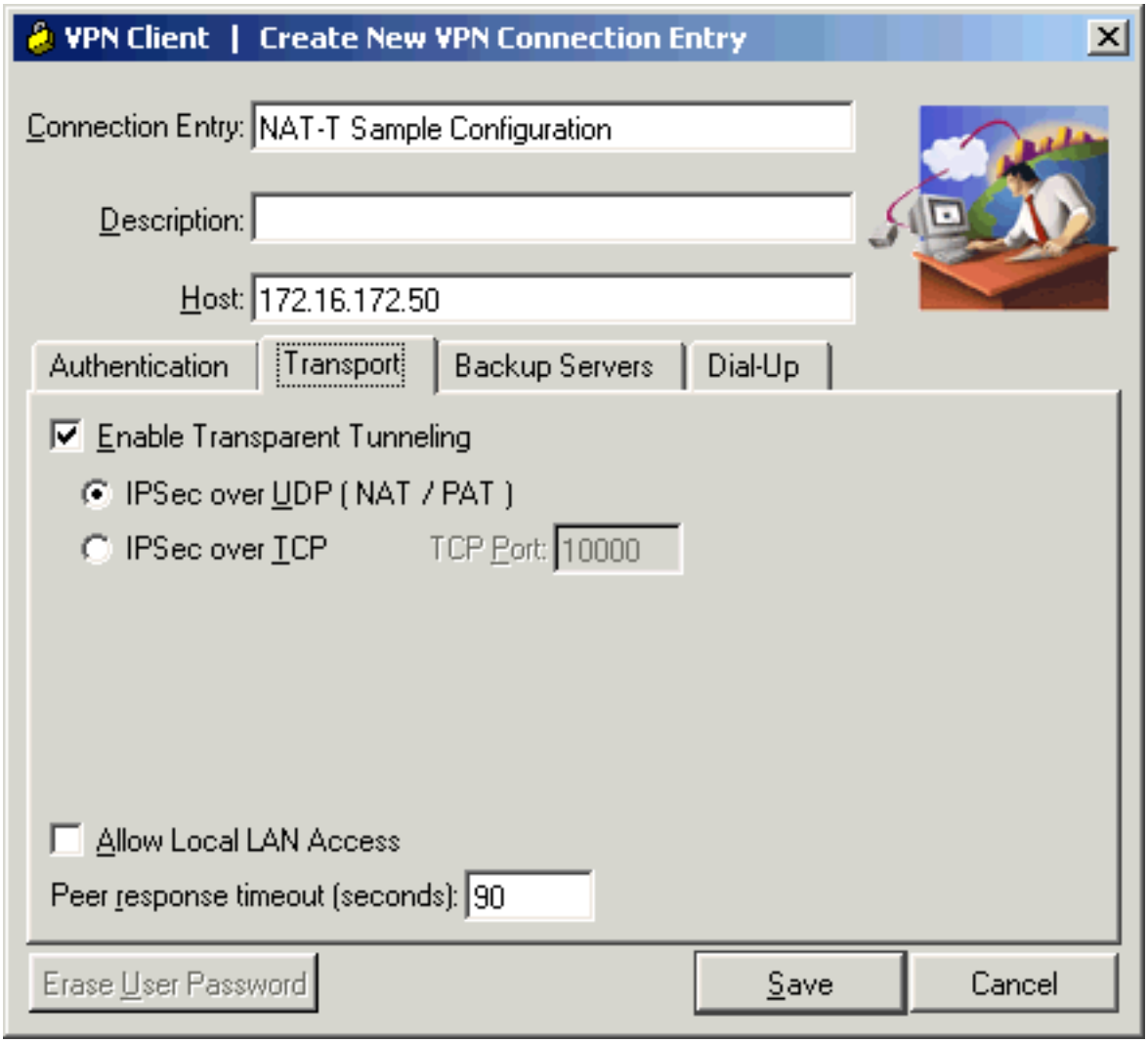
VPN Concentrator 버전 4.1 이상에서 NAT-T를 활성화하려면 Configuration(컨피그레이션) > Tunneling and **Security(터널링 및 보안) > IPSec > NAT Transparency(NAT 투명도)를** 선택하여 동일한 NAT Transparency(NAT 투명도) 창으로 이동합니다.



VPN 클라이언트 구성

NAT-T를 사용하려면 Enable **Transparent Tunneling을 선택합니다**. 다음 예는 버전 4.0 이상의 VPN 클라이언트에서 이 방법을 보여줍니다.

참고: VPN Client 버전 3.x에서 동일한 구성 옵션을 사용할 수 있습니다.



다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

일부 **show 명령은** 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show 명령 출력의 분석 결과를 볼 수 있습니다.**

추가 문제 해결 정보는 IP Security Troubleshooting - Understanding and Using debug Commands(IP 보안 문제 해결 - 디버그 명령 이해 및 사용)에서 확인할 수 있습니다.

PIX 컨피그레이션 확인

다음 명령은 PIX 컨피그레이션을 확인하는 데 사용됩니다.

- **show xlate** - 아래 출력에 표시된 대로 PIX는 두 VPN 클라이언트에 대해 서로 다른 소스 포트를 사용하지만 대상 포트는 동일합니다. 모든 IPSec 데이터 패킷은 UDP 포트 4500을 사용하여 래핑됩니다. 후속 키 재지정 협상에서는 동일한 소스 및 대상 포트도 사용합니다.

```
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)
```

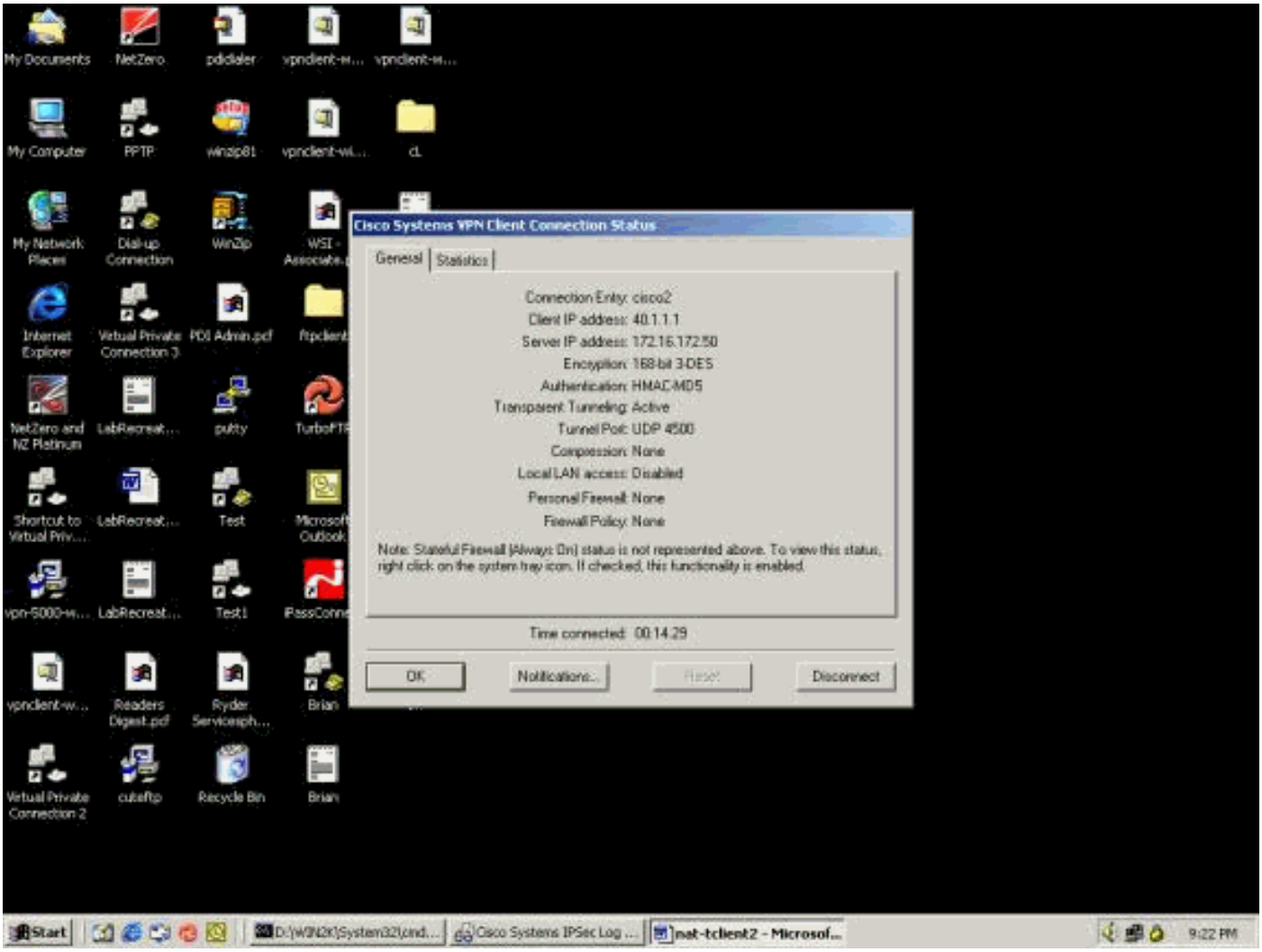
- **show arp** - 이 명령을 사용하여 ARP(Address Resolution Protocol) 테이블을 표시하고 ARP 요

청이 처리되는지 확인합니다.

```
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 클라이언트 통계

VPN 터널이 설정되면 노란색 잠금을 마우스 오른쪽 버튼으로 클릭하고 **Status**(상태)를 선택합니다. 유사한 창이 아래에 나와 있습니다. 터널 포트는 NAT-T를 사용 중임을 나타내는 UDP 4500입니다.

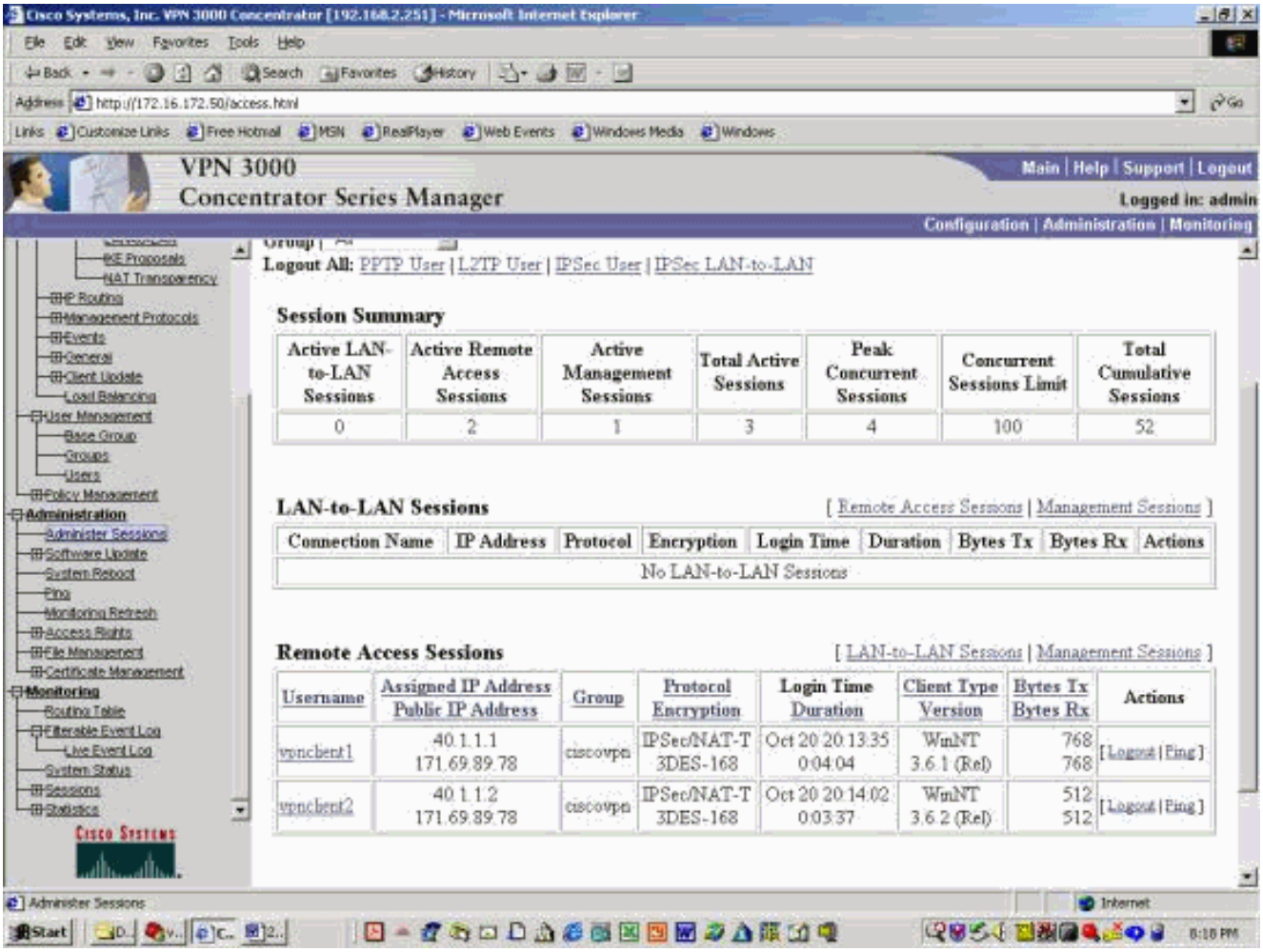


VPN Concentrator 통계

다음 단계를 완료하십시오.

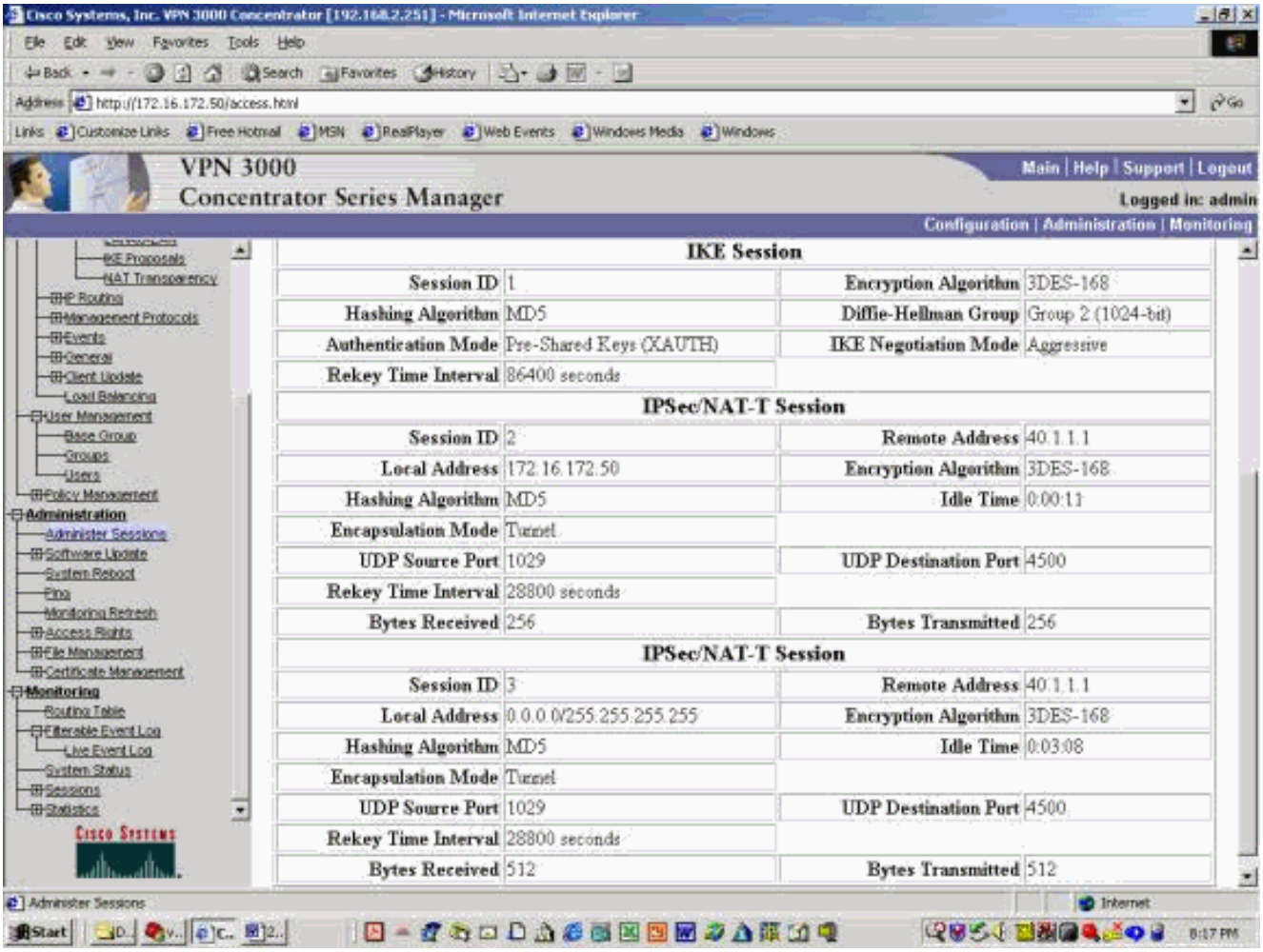
1. VPN Concentrator에서 Administration(관리) **> Administrator Session(관리자 세션)을** 선택합니다.VPN 클라이언트 세션은 Remote Access Sessions(원격 액세스 세션)에서 확인할 수 있습니다. 아래 예는 VPN Concentrator에 대한 IPSec 터널을 설정한 후 두 클라이언트의 세션을 보여줍니다. 둘 다 공용 IP 주소 171.69.89.78을 사용하고 있으며 40.1.1.1 및 40.1.1.2이 할당되었습니다

.



2. 클라이언트 사용자 이름을 두 번 클릭합니다.IPSec/IKE 통계가 아래 예와 같이 표시됩니다. 클라이언트에서 사용하는 UDP 소스 포트는 1029이고 사용된 대상 포트는 4500입니다

.



문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

참고: debug 명령을 실행하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

참고: 추가 PIX 문제 해결 정보는 IP 보안 문제 해결 - 디버그 명령 이해 및 사용에서 확인할 수 있습니다.

VPN 클라이언트 로그

VPN 클라이언트가 설치된 PC에서 VPN Concentrator에 대한 연결을 설정하기 전에 로그 뷰어를 엽니다. 이 로그 출력에서는 NAT 관련 메시지를 강조 표시합니다.

```
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 Concentrator 로그

VPN Concentrator의 로그를 보려면 **Monitoring > Filterable Event Log**를 선택하고 Event Classes IKE, **IKEDBG, IKEDECODE** 및 **IPSECDBG**와 Severity 1~13을 선택합니다.

```
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
```

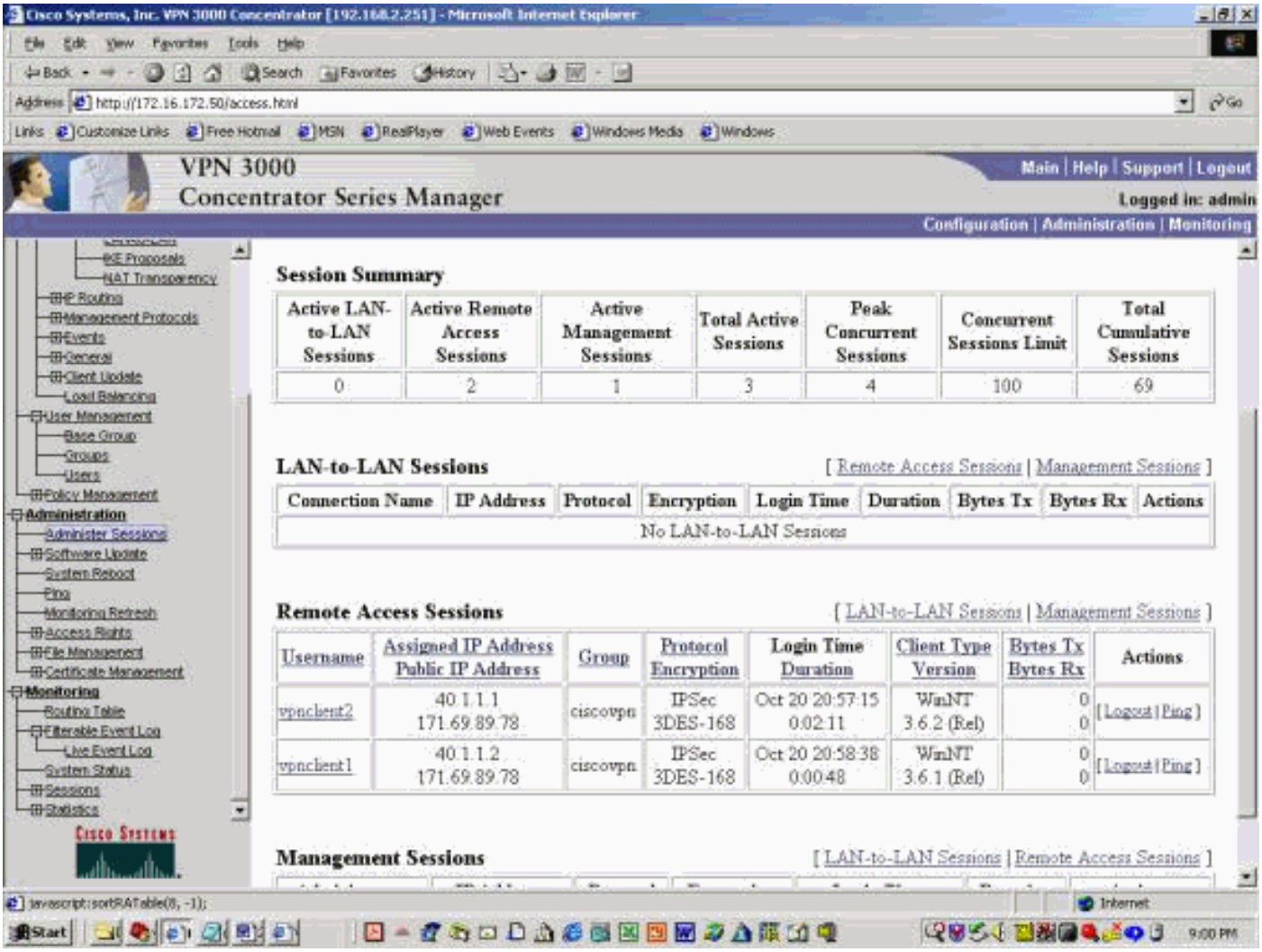
```
ISAKMP HEADER : ( Version 1.0 )
  Initiator Cookie(8): C5 A0 F0 8B 69 60 D7 47
  Responder Cookie(8): 48 65 B1 6F 36 1F 9D 3A
  Next Payload  :HASH (8)
  Exchange Type :Oakley Informational
  Flags         :1   (ENCRYPT )
3073 10/20/2002 20:23:42.470 SEV=8 IKEDECODE/0 RPT=8204 171.69.89.78
  Message 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
```

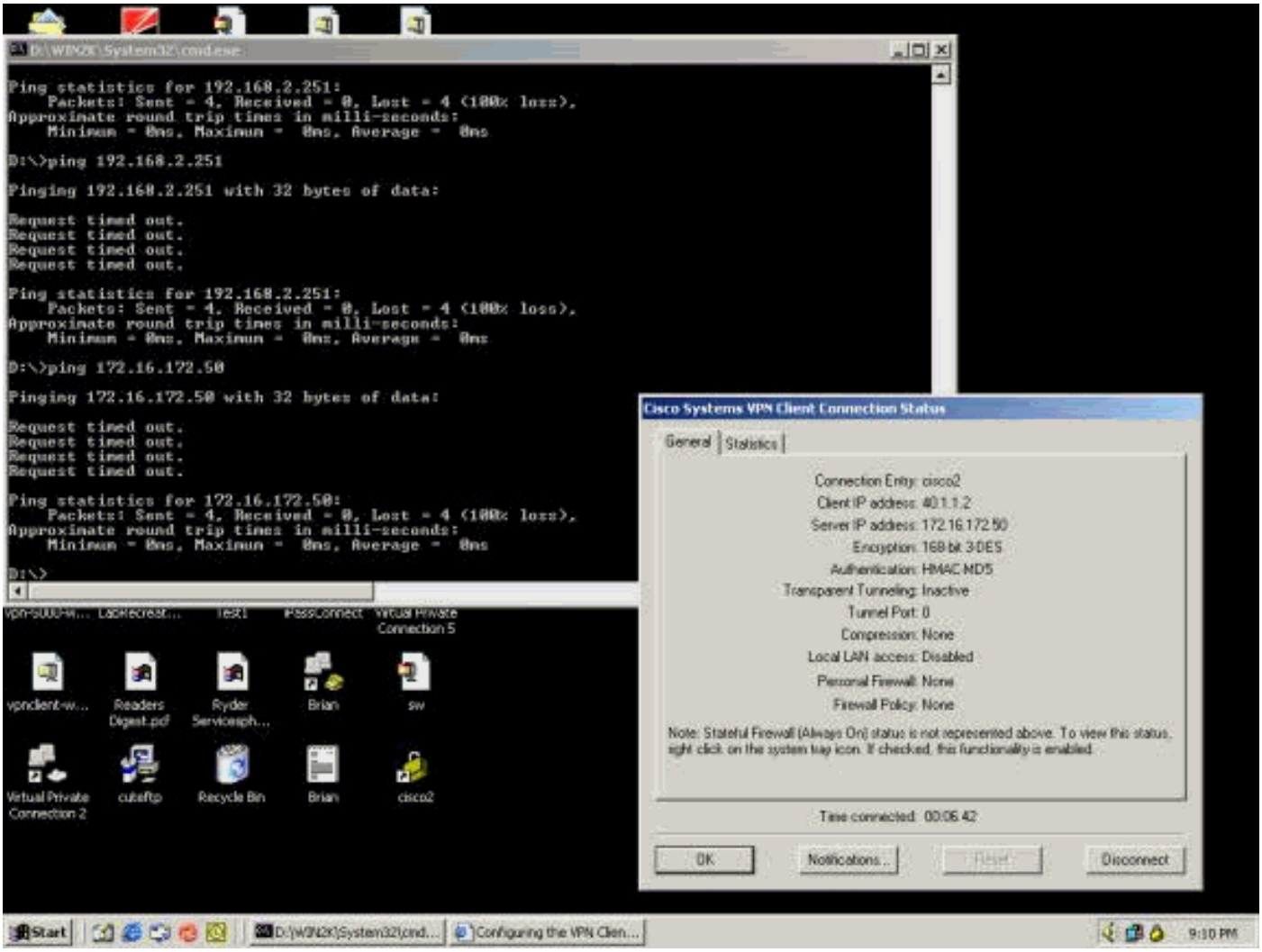
추가 문제 해결

NAT-T는 포트 4500을 사용하여 UDP 데이터그램에서 IPSec 트래픽을 캡슐화합니다. VPN Concentrator에서 NAT-T를 선택하지 않거나 VPN 클라이언트에서 NAT 투명도를 선택하지 않으면 IPSec 터널이 설정됩니다. 그러나 데이터를 전달할 수는 없습니다. NAT-T가 작동하려면 Concentrator에서 NAT-T를 확인하고 클라이언트에서 NAT 투명도(over UDP)를 선택해야 합니다.

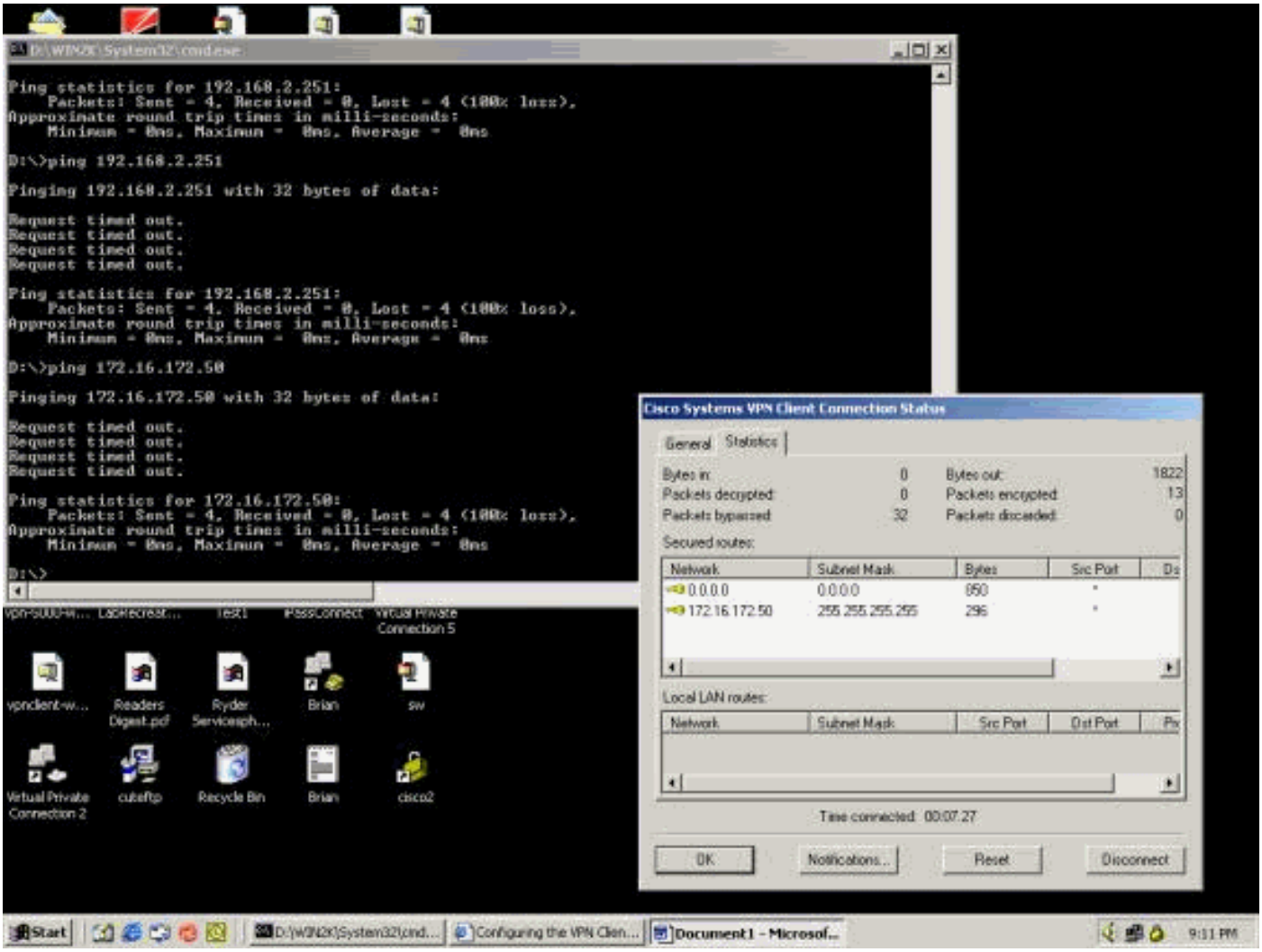
아래 예는 Concentrator에서 NAT-T를 선택하지 않은 사례를 보여줍니다. 클라이언트에서 투명 터널링이 확인되었습니다. 이 경우 클라이언트와 Concentrator 간에 IPSec 터널이 설정됩니다. 그러나 IPSec 터널 포트 협상이 실패했으므로 클라이언트와 Concentrator 간에 데이터가 전달되지 않습니다. 따라서 원격 액세스 세션에 대해 전송 및 수신된 바이트는 0입니다.



아래 예는 VPN 클라이언트의 통계를 보여줍니다. 협상된 터널 포트는 0입니다. DOS 프롬프트에서 192.168.2.251(VPN 3000 Concentrator의 전용 인터페이스) 및 172.16.172.50을 ping하려고 시도합니다. 그러나 터널 포트가 협상되지 않아 IPSec 데이터가 원격 VPN 서버에서 삭제되기 때문에 이러한 ping은 실패합니다.



아래 예는 VPN 클라이언트가 암호화된 데이터(13개의 패킷)를 전송하고 있음을 보여줍니다. 그러나 원격 VPN 서버에 대해 해독된 패킷 수는 0이며 암호화된 데이터를 다시 전송하지 않았습니다. 협상된 터널 포트가 없으므로 원격 VPN 서버는 패킷을 폐기하고 응답 데이터를 보내지 않습니다.



관련 정보

- Cisco VPN 3000 Series Concentrator 지원 페이지
- Cisco VPN 3000 Series 클라이언트 지원 페이지
- IPSec 지원 페이지
- 기술 지원 및 문서 – Cisco Systems