

NATトラバーサルを使用したCisco VPN 3000 コンセントレータへの複数VPNクライアント設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[ネットワーク図](#)

[表記法](#)

[背景説明](#)

[PIX の設定](#)

[VPN 3000 コンセントレータの設定](#)

[VPN クライアントの設定](#)

[確認](#)

[PIX 設定の検証](#)

[VPN クライアントの統計情報](#)

[VPN コンセントレータの統計情報](#)

[トラブルシューティング](#)

[VPN クライアント ログ](#)

[VPN コンセントレータ ログ](#)

[その他のトラブルシューティング](#)

[関連情報](#)

概要

この文書では、Port Address Translation (PAT; ポート アドレス変換) /Network Address Translation (NAT; ネットワーク アドレス変換) デバイスの背後に設置された Cisco VPN クライアントと、リモート Cisco VPN コンセントレータ間での NAT Traversal (NAT-T) の設定方法について説明します。NAT-T は、VPN クライアントと VPN コンセントレータ間、または NAT/PAT デバイスの背後のコンセントレータ間で使用できます。また、NAT-T は、Cisco IOS® ソフトウェアと PIX Firewall を実行する Cisco ルータに接続するときに使用できます。ただし、これらの設定はこのドキュメントに記載されていません。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco VPN 3000 コンセントレータ 4.0(1)B
- Cisco VPN クライアント3.6.1 および 4.0(3) Rel
- Cisco PIX ファイアウォール (PAT デバイス) バージョン 6.3(3)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



PIX ファイアウォールの背後の 2 台の PC (10.10.10.2 と 10.10.10.3) で、VPN クライアントが設定されています。このシナリオのPIXは単にPATデバイスとして使用され、171.69.89.78へのPATを実行します。複数の内部接続をPATできるデバイスは172.16.172.50です。VPN 3000コンセントレータのパブリックアドレスはです。次の例では、NAT-Tがのこのネゴシエーションの使用を使用使用します。

表記法

ドキュメント表記の詳細は、「[シスコテクニカルティップスの表記法](#)」を参照してください。

背景説明

NAT-T ネゴシエーションが終了すると、発信側はランダムな User Datagram Protocol (UDP; ユーザデータグラムプロトコル) ポート (Y) を使用できます。宛先ポートは、UDP (Y, 4500) であるように、UDP 4500 である必要があり、応答側は UDP (4500, Y) を使用します。以降のすべての Internet Key Exchange (IKE; インターネット鍵交換) ネゴシエーションと鍵の再生成は、これらのポートで実行されます。NAT-T ネゴシエーション中、両方の IPsec ピアが UDP ポートをネゴシエートし、ピアが NAT/PAT デバイスの背後にあるかどうかも決定されます。NAT/PAT デバイスの背後の IPsec ピアは、IPsec-over-UDP NAT キープアライブ パケットを、NAT/PAT デバイスの背後にない IPsec ピアに送信します。NAT-T はポート 4500 を使って IPsec トラフィックを UDP ダイアグラムにカプセル化し、NAT デバイスにポート情報を提供します。NAT-T によって NAT デバイスが自動検出され、必要な場合だけ、IPsec トラフィックがカプセル化されます。

VPN 3000 コンセントレータに IPsec over NAT 変換を実装した場合、IPsec over TCP が最優先となり、次が NAT-T、その次が IPsec over UDP となります。デフォルトでは NAT-T はオフになります。Tunneling Protocols の下にある IPsec configuration の NAT Transparency にあるチェッ

クボックスを使って、NAT-T をイネーブルにする必要があります。また、LAN-to-LAN トンネルの場合、LAN-to-LAN configurations IPsec NAT-T フィールドの下にある NAT-T をオンにする必要があります。

NAT-T を使用するには、次のステップを実行する必要があります。

1. VPN コンセントレータの前に設定したファイアウォールのポート 4500 をオープンします。
2. ポート 4500 を使って、以前の IPsec/UDP 設定を別のポートに再設定します。
3. **[Configuration] > [Interfaces] > [Ethernet]**の順に選択し、**[Fragmentation Policy]**パラメータの2番目または3番目のオプションを選択します。これらのオプションを使用すると、IPフラグメンテーションをサポートしていないNATデバイスをトラフィックが通過できます。IPフラグメンテーションをサポートするNATデバイスの動作を妨げるものではありません。

PIX の設定

PIX に関連する設定の出力を次に示します。

```
PIX ファイアウォール

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:6990adf6e0e2800ed409ae7364eccc9d
: end

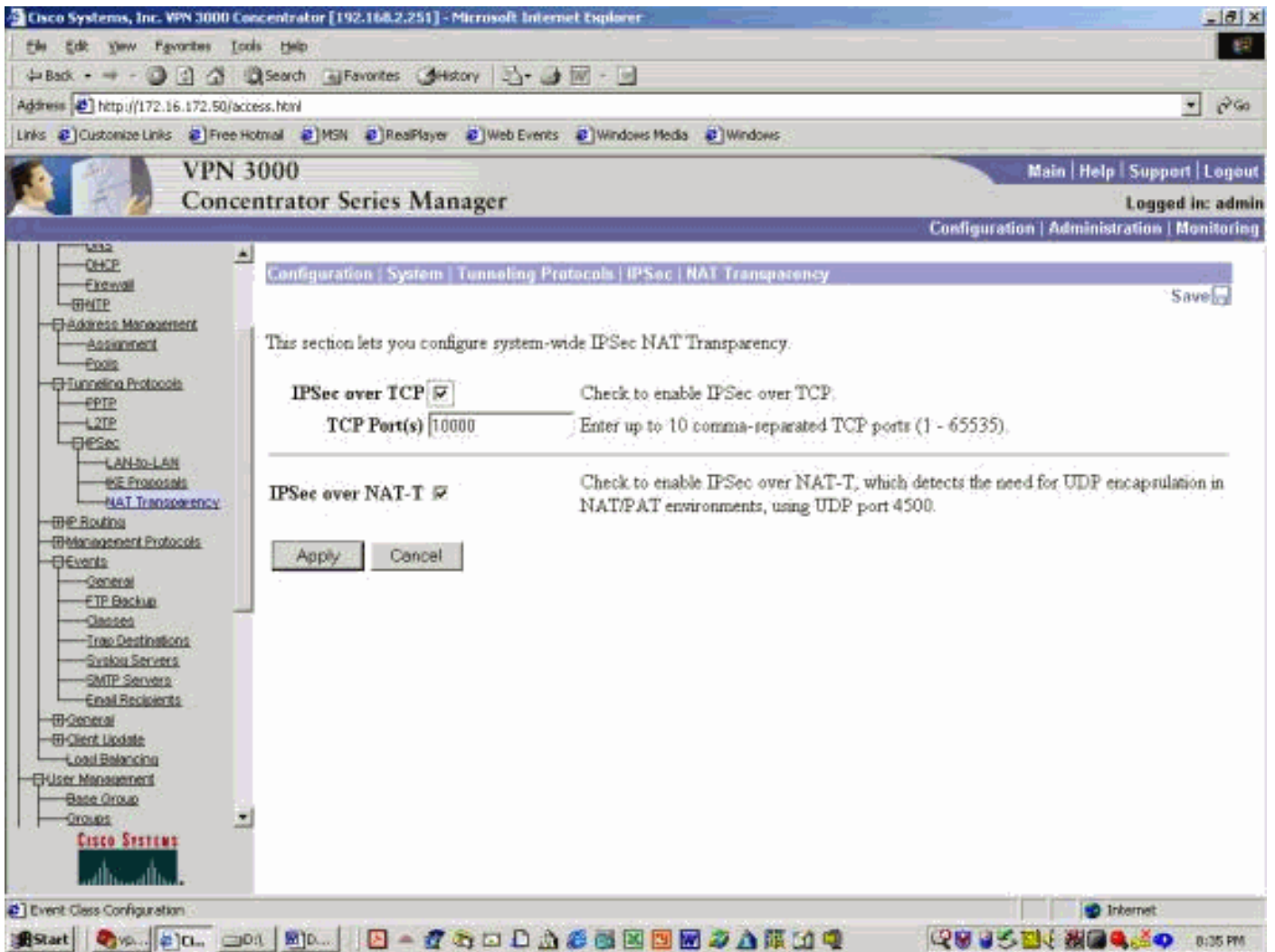
[OK]
```

VPN 3000 コンセントレータの設定

この設定例では、VPN 3000 コンセントレータがすでに IP 接続用に設定され、標準の (NAT-T に対応していない) VPN 接続が確立済みであるものとします。

バージョン4.1より前のVPN 3000コンセントレータリリースでNAT-Tを有効にするには、**Configurations > System > Tunneling protocols > IPsec > NAT Transparency**の順に選択し、次の例に示すようにコンセントレータで**IPSEC OVER NAT-Tオプション**ををチェックします。NAT-T オプションはデフォルトではオフです。

VPNコンセントレータバージョン4.1以降でNAT-Tを有効にするには、**Configuration > Tunneling and Security > IPsec > NAT Transparency**の順に選択して、同じNAT Transparencyウィンドウに移動します。



VPN クライアントの設定

NAT-T を使用するには、Enable Transparent Tunneling をオンにします。次の例は、バージョン 4.0 以降の VPN クライアントでの例を示します。

注：VPN Clientバージョン3.xでも同じ設定オプションを使用できます。

VPN Client | Create New VPN Connection Entry

Connection Entry: NAT-T Sample Configuration

Description:

Host: 172.16.172.50

Authentication | **Transport** | Backup Servers | Dial-Up

Enable Transparent Tunneling

IPSec over UDP (NAT / PAT)

IPSec over ICP TCP Port: 10000

Allow Local LAN Access

Peer response timeout (seconds): 90

Erase User Password Save Cancel

確認

ここでは、設定が正しく機能していることを確認するために使用する情報を示します。

一部の show コマンドは[アウトプット インタープリタ ツール](#)によってサポートされています ([登録ユーザ専用](#))。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

追加のトラブルシューティング情報は、「[IP セキュリティのトラブルシューティング - debug コマンドの理解と使用](#)」を参照してください。

PIX 設定の検証

次のコマンドを使って、PIX 設定を検証します。

- **show xlate** : 次の出力に示すように、PIXは2つのVPN Clientに異なる送信元ポートを使用していますが、宛先ポートは同じです。すべての IPSec データ パケットは、UDP ポート 4500 を使ってラップされています。以降、鍵の再生成のネゴシエーションを実行しても、同じ送信元ポートと宛先ポートが使用されます。

```
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)
```

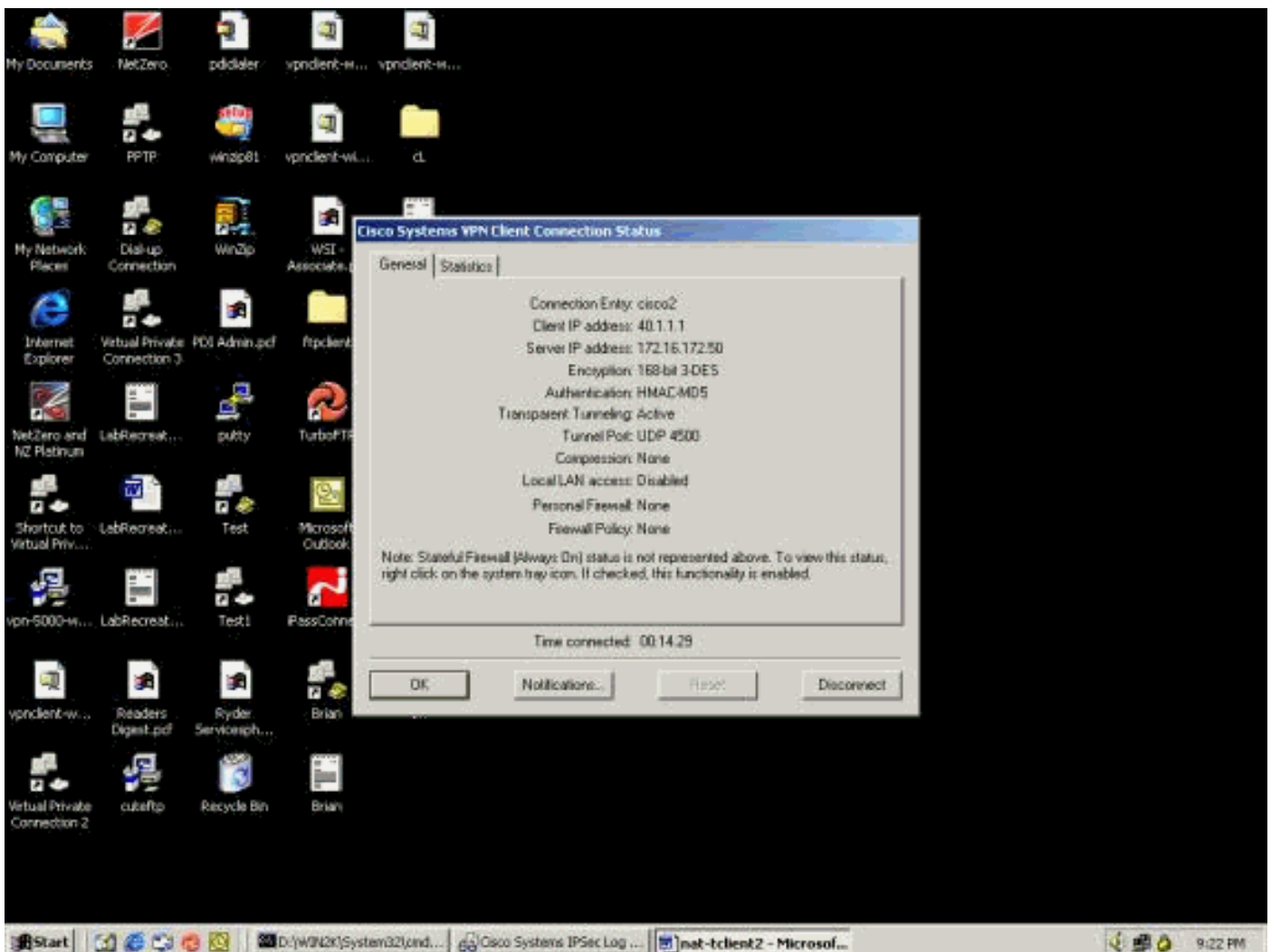
PAT Global 171.69.89.78(4) Local 10.10.10.2(500)

- **show arp** : このコマンドを使用して、アドレス解決プロトコル(ARP)テーブルを表示し、ARP要求が処理されているかどうかを確認します。

```
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 クライアントの統計情報

VPN トンネルの確立後、黄色の鍵を右クリックし、Status を選択します。同じようなウィンドウを次に示します。トンネル ポートは UDP 4500 であるという点に注意してください。このことから、NAT-T が使用されていることがわかります。



VPN コンセントレータの統計情報

次のステップを実行します。

1. VPN コンセントレータで、[Administration] > [Administrator Session] の順に選択します。VPN クライアント セッションが、Remote Access Sessions の下に表示されます。次の例は、VPN コンセントレータへの IPSec トンネルを確立した後の 2 台のクライアントのセッションを示しています。これらのクライアントは両方ともパブリック IP アドレス

171.69.89.78 を使用しており、40.1.1.1 と 40.1.1.2 がそれぞれ割り当てられています。

Group: [PPTP User](#) | [L2TP User](#) | [IPsec User](#) | [IPsec LAN-to-LAN](#)

Session Summary

Active LAN-to-LAN Sessions	Active Remote Access Sessions	Active Management Sessions	Total Active Sessions	Peak Concurrent Sessions	Concurrent Sessions Limit	Total Cumulative Sessions
0	2	1	3	4	100	52

LAN-to-LAN Sessions [[Remote Access Sessions](#) | [Management Sessions](#)]

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx	Actions
No LAN-to-LAN Sessions								

Remote Access Sessions [[LAN-to-LAN Sessions](#) | [Management Sessions](#)]

Username	Assigned IP Address Public IP Address	Group	Protocol Encryption	Login Time Duration	Client Type Version	Bytes Tx Bytes Rx	Actions
vpnclient1	40.1.1.1	ciscovpn	IPsec/NAT-T 3DES-168	Oct 20 20 13:35 0:04:04	WinNT 3.6.1 (Rel)	768 768	[Logout] [Eing]
	171.69.89.78						
vpnclient2	40.1.1.2	ciscovpn	IPsec/NAT-T 3DES-168	Oct 20 20 14:02 0:03:37	WinNT 3.6.2 (Rel)	512 512	[Logout] [Eing]
	171.69.89.78						

2. クライアント ユーザ名をダブルクリックします。次の例のように、IPsec/IKE 統計情報が表示されます。クライアントが使用する UDP 送信元ポートは 1029 で、宛先ポートは 4500 です。

The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface. The browser window title is "Cisco Systems, Inc. VPN 3000 Concentrator [192.168.2.251] - Microsoft Internet Explorer". The address bar shows "http://172.16.172.50/access.html". The page title is "VPN 3000 Concentrator Series Manager". The user is logged in as "admin". The interface is divided into three main sections: Administration, Monitoring, and Configuration. The Administration section is currently selected, and the "Administer Sessions" link is active. The main content area displays the following session details:

IKE Session			
Session ID	1	Encryption Algorithm	3DES-168
Hashing Algorithm	MD5	Diffie-Hellman Group	Group 2 (1024-bit)
Authentication Mode	Pre-Shared Keys (XAUTH)	IKE Negotiation Mode	Aggressive
Rekey Time Interval	86400 seconds		
IPSec/NAT-T Session			
Session ID	2	Remote Address	40.1.1.1
Local Address	172.16.172.50	Encryption Algorithm	3DES-168
Hashing Algorithm	MD5	Idle Time	0:00:11
Encapsulation Mode	Tunnel		
UDP Source Port	1029	UDP Destination Port	4500
Rekey Time Interval	28800 seconds		
Bytes Received	256	Bytes Transmitted	256
IPSec/NAT-T Session			
Session ID	3	Remote Address	40.1.1.1
Local Address	0.0.0.0/255.255.255.255	Encryption Algorithm	3DES-168
Hashing Algorithm	MD5	Idle Time	0:03:08
Encapsulation Mode	Tunnel		
UDP Source Port	1029	UDP Destination Port	4500
Rekey Time Interval	28800 seconds		
Bytes Received	512	Bytes Transmitted	512

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

注：debugコマンドを発行する前に、『[debugコマンドの重要な情報](#)』を参照してください。

注：追加のPIXのトラブルシューティング情報は、『[IP Securityのトラブルシューティング - debugコマンドの理解と使用](#)』を参照してください。

VPN クライアント ログ

VPN ClientがインストールされているPCで、VPNコンセントレータへの接続を確立する前にLog Viewerを開きます。このログ出力は、NAT-T固有のメッセージを強調表示します。

```

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 コンセントレータ ログ

VPNコンセントレータのログを表示するには、Monitoring > Filterable Event Logの順に選択し、Event Classes IKE, IKEDBG, KEDECODE, and IPSECDBG with Severities 1 ~ 13.

```

2835 10/20/2002 20:22:42.390 SEV=8 IKEDCODE/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, hashKeyLen 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, hashKeyLen 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, hashKey
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: rcv 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: rcv 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 IKEDCODE/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 IKEDCODE/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

```

その他のトラブルシューティング

NAT-T は、ポート 4500 を使って、IPSec トラフィックを UDP データグラムにカプセル化します。VPN コンセントレータで NAT-T がチェックされていない場合、または VPN Client で NAT 透過がチェックされていない場合、IPSec トンネルが確立されます。ただし、データを渡すことはできません。NAT-T を動作させるには、コンセントレータで NAT-T をオンにし、(UDP を介して) クライアントで NAT transparency をオンにする必要があります。

次の例は、コンセントレータで NAT-T がオンになっていなかった場合を示しています。クライアントでは、Transparent Tunneling がオンになっていました。この場合、クライアントとコンセントレータ間で IPSec トンネルが確立されます。ただし、IPSec トンネル ポート ネゴシエーションが失敗したため、クライアントとコンセントレータ間でデータは受け渡されません。そのため、リモート アクセス セッションに対して送受信されたバイト数は 0 になります。

The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface. The left sidebar contains a navigation tree with categories like IPsec, User Management, Administration, and Monitoring. The main content area displays three session summary tables:

Session Summary

Active LAN-to-LAN Sessions	Active Remote Access Sessions	Active Management Sessions	Total Active Sessions	Peak Concurrent Sessions	Concurrent Sessions Limit	Total Cumulative Sessions
0	2	1	3	4	100	69

LAN-to-LAN Sessions [Remote Access Sessions | Management Sessions]

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx	Actions
No LAN-to-LAN Sessions								

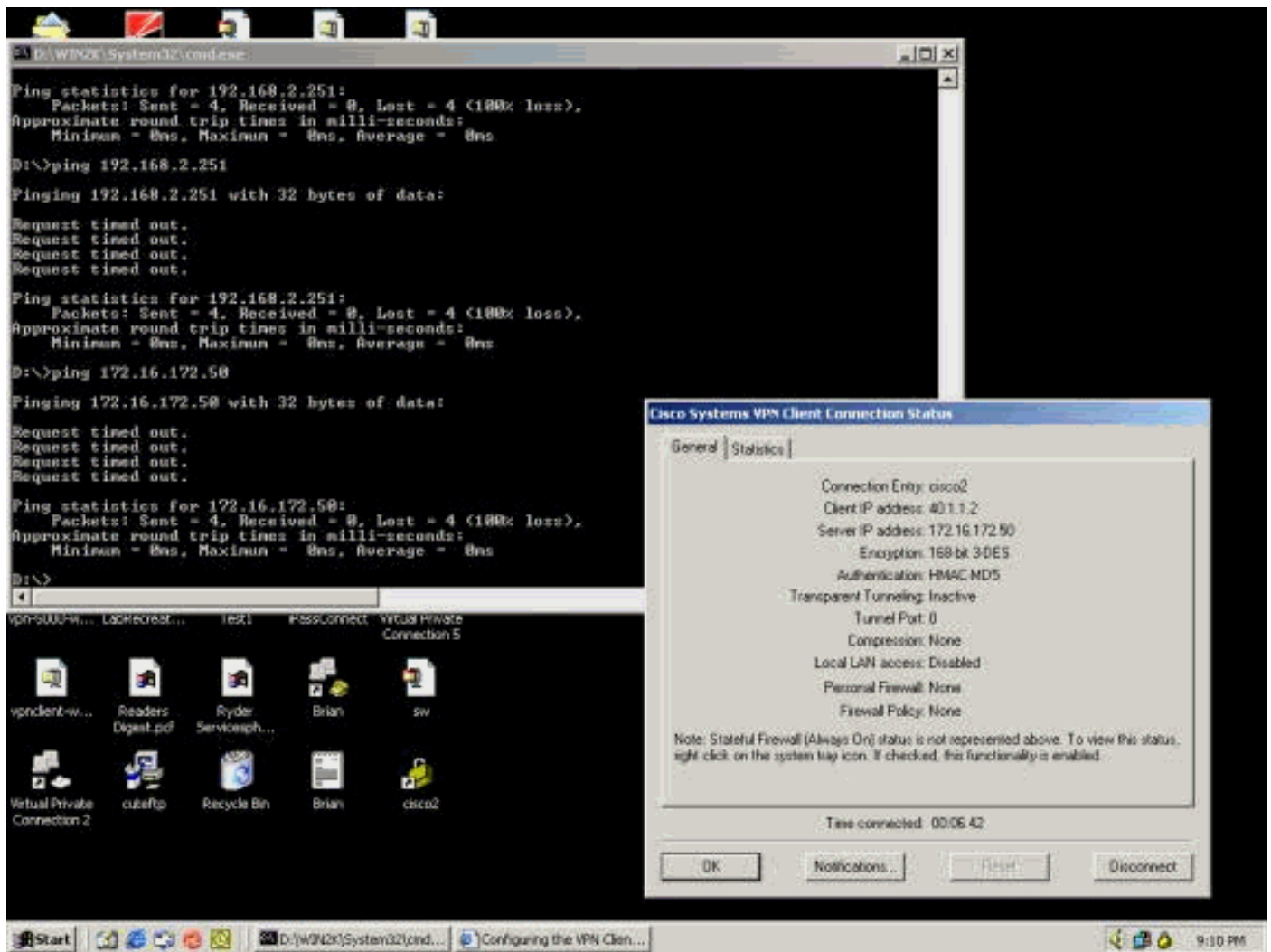
Remote Access Sessions [LAN-to-LAN Sessions | Management Sessions]

Username	Assigned IP Address Public IP Address	Group	Protocol Encryption	Login Time Duration	Client Type Version	Bytes Tx Bytes Rx	Actions
vpnclient2	40.1.1.1	ciscovpn	IPSec 3DES-168	Oct 20 20:57:15	WinNT 3.6.2 (Rel)	0	[Logout Ping]
	171.69.89.78			00:2:11		0	
vpnclient1	40.1.1.2	ciscovpn	IPSec 3DES-168	Oct 20 20:58:38	WinNT 3.6.1 (Rel)	0	[Logout Ping]
	171.69.89.78			00:0:48		0	

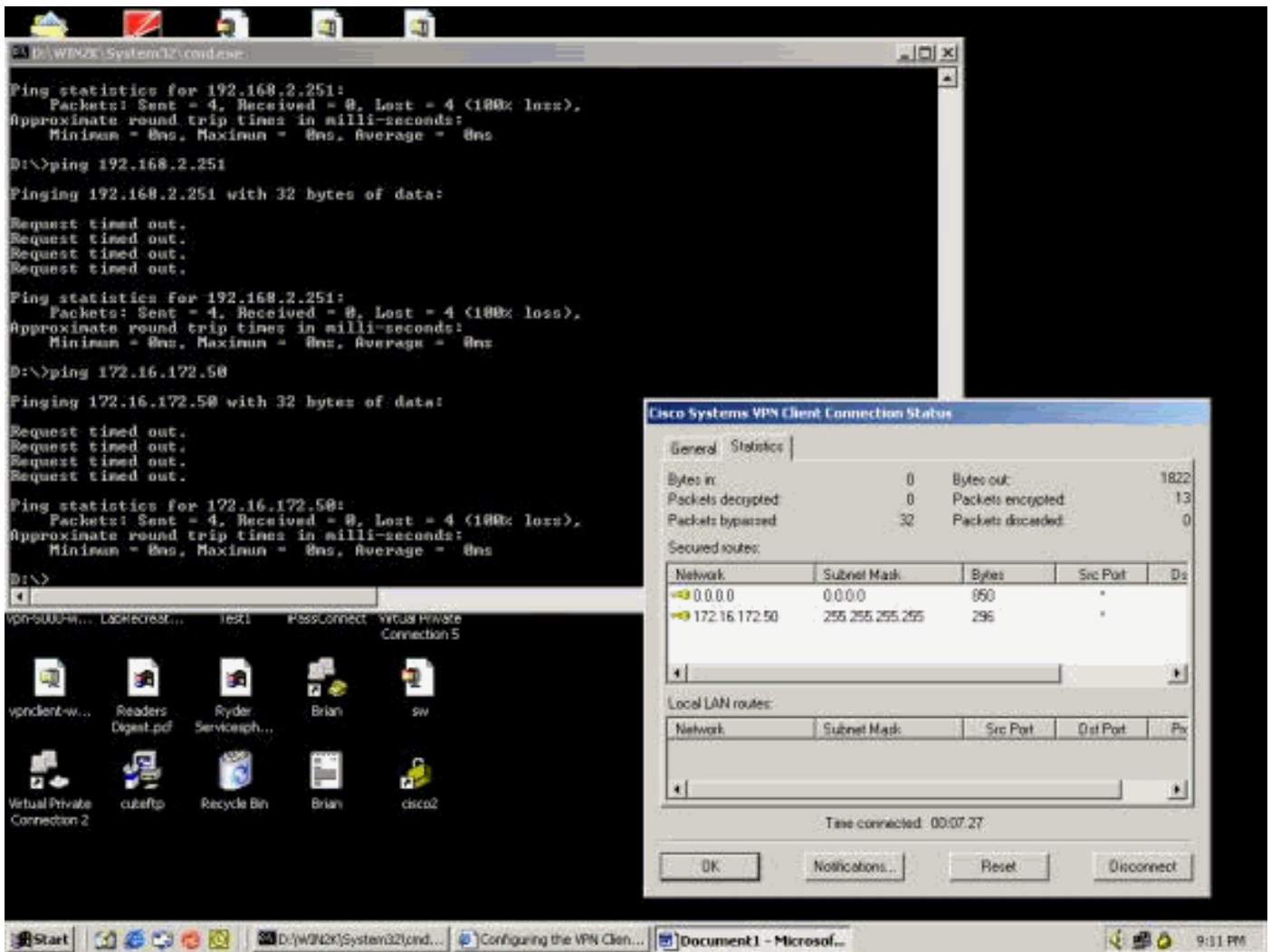
Management Sessions [LAN-to-LAN Sessions | Remote Access Sessions]

次の例は、VPN クライアントの統計情報を示しています。ネゴシエートされたトンネルポートが 0 であることに注意してください。DOS プロンプトから 192.168.2.251 (VPN 3000 コンセントレータのプライベートインターフェイス) および 172.16.172.50 に対して ping を実行します。しかし

、トンネルポートのネゴシエーションが実行されていなかったため、これらの pings は失敗し、IPSec データは、リモート VPN サーバで破棄されます。



次の例は、VPN クライアントが、暗号化データ (13 パケット) を送信していることを示しています。しかし、リモート VPN サーバへの暗号化パケットの数は 0 で、リモート VPN サーバは暗号化データを送り返していません。これは、トンネルポートがネゴシエートされていないため、リモート VPN サーバがパケットを破棄し、応答データを送信しないためです。



関連情報

- [Cisco VPN 3000 シリーズ コンセントレータに関するサポート ページ](#)
- [Cisco VPN 3000 シリーズ クライアントに関するサポート ページ](#)
- [IPSec に関するサポート ページ](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)