# Configuration de plusieurs clients VPN sur un concentrateur Cisco VPN 3000 à l'aide de NAT-Traversal

## Contenu



## Introduction

Ce document affiche comment configurer une traversée de traduction d'adresses réseau (NAT-T) entre les Clients VPN Cisco situés derrière un périphérique de translation d'adresses d'adresse du port (PAT) /NAT et un concentrateur distant de Cisco VPN. NAT-T peut être utilisé entre les clients vpn et un concentrateur VPN, ou entre les concentrateurs derrière un périphérique NAT/PAT. NAT-T peut également être utilisé en connectant au Cisco IOS® de routeur de Cisco un logiciel courant et le Pare-feu PIX ; cependant, ces configurations ne sont pas discutées dans ce document.

## Conditions préalables

### Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

## Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Concentrateur 4.0(1)B de Cisco VPN 3000
- Clients VPN Cisco : 3.6.1 et 4.0(3) version
- Version 6.3(3) de Pare-feu de Cisco PIX (périphérique de TAPOTEMENT)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

## Diagramme du réseau

Ce document utilise la configuration réseau suivante :


Il y a des clients vpn sur les deux PC (10.10.10.2 et 10.10.10.3) derrière le Pare-feu PIX. Le PIX dans ce scénario simplement est utilisé en tant qu'un périphérique de PAT, et attitudes PAT sur ces adresses à 171.69.89.78. N'importe quel périphérique qui peut TAPOTER de plusieurs connexions internes peut être utilisé ici. L'annonce publique de concentrateur VPN 3000 est 172.16.172.50. L'exemple suivant explique comment configurer les clients et le concentrateur de sorte que NAT-T soit utilisé pendant la négociation d'IKE.

## Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

# Informations générales

Après que la négociation NAT-T soit terminée, le demandeur peut utiliser n'importe quel port aléatoire de Protocole UDP (User Datagram Protocol) (y). La destination port doit être l'UDP 4500, comme dans l'UDP (Y, 4500), et le responder utilise l'UDP (4500, Y). Toutes les négociations ultérieures d'Échange de clés Internet (IKE) et la nouvelle saisie sont faites sur ces ports. Pendant les négociations NAT-T, les les deux les pairs d'IPSec négocient les ports UDP et déterminent également s'ils sont derrière un périphérique NAT/PAT. Le pair d'IPSec derrière le périphérique NAT/PAT envoie au l'IPSec-au-dessus-UDP le paquet keepalive NAT au pair d'IPSec qui n'est pas derrière un périphérique NAT/PAT. NAT-T encapsule le trafic d'IPSec dans les datagrammes UDP, utilisant le port 4500, fournissant de ce fait aux périphériques NAT les informations de port. NAT-T autodetects tous les périphériques NAT, et encapsule seulement le trafic d'IPSec si

nécessaire.

En mettant en application IPSec au-dessus de la traduction NAT sur le concentrateur VPN 3000, IPSec au-dessus de TCP prend la premiers priorité, puis NAT-T, et puis IPSec au-dessus de l'UDP. Par défaut, NAT-T est arrêté. Vous devez activer NAT-T utilisant une case à cocher située dans la transparence NAT, sous la configuration IPSec située sous des protocoles de Tunnellisation. En outre, pour un tunnel entre réseaux locaux, vous devez tourner NAT-T en fonction sous le champ d'IPSec NAT-T de configurations entre réseaux locaux.

Pour utiliser NAT-T, vous devez se terminer ces étapes :

1. Port ouvert 4500 sur tout Pare-feu que vous avez configuré devant un concentrateur VPN.
2. Modifiez les configurations précédentes IPSec/UDP utilisant le port 4500 à un port différent.
3. Choisissez le **Configuration > Interfaces > les Ethernets**, et choisissez les deuxièmes ou troisième options pour le paramètre de stratégie de fragmentation.Ces options permettent au trafic pour voyager à travers les périphériques NAT qui ne prennent en charge pas la fragmentation IP ; ils n'empêchent pas le fonctionnement des périphériques NAT qui prennent en charge la fragmentation IP.

## Configurez le PIX

La sortie de configuration appropriée pour le PIX est affichée ici :

**Pare-feu PIX**

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

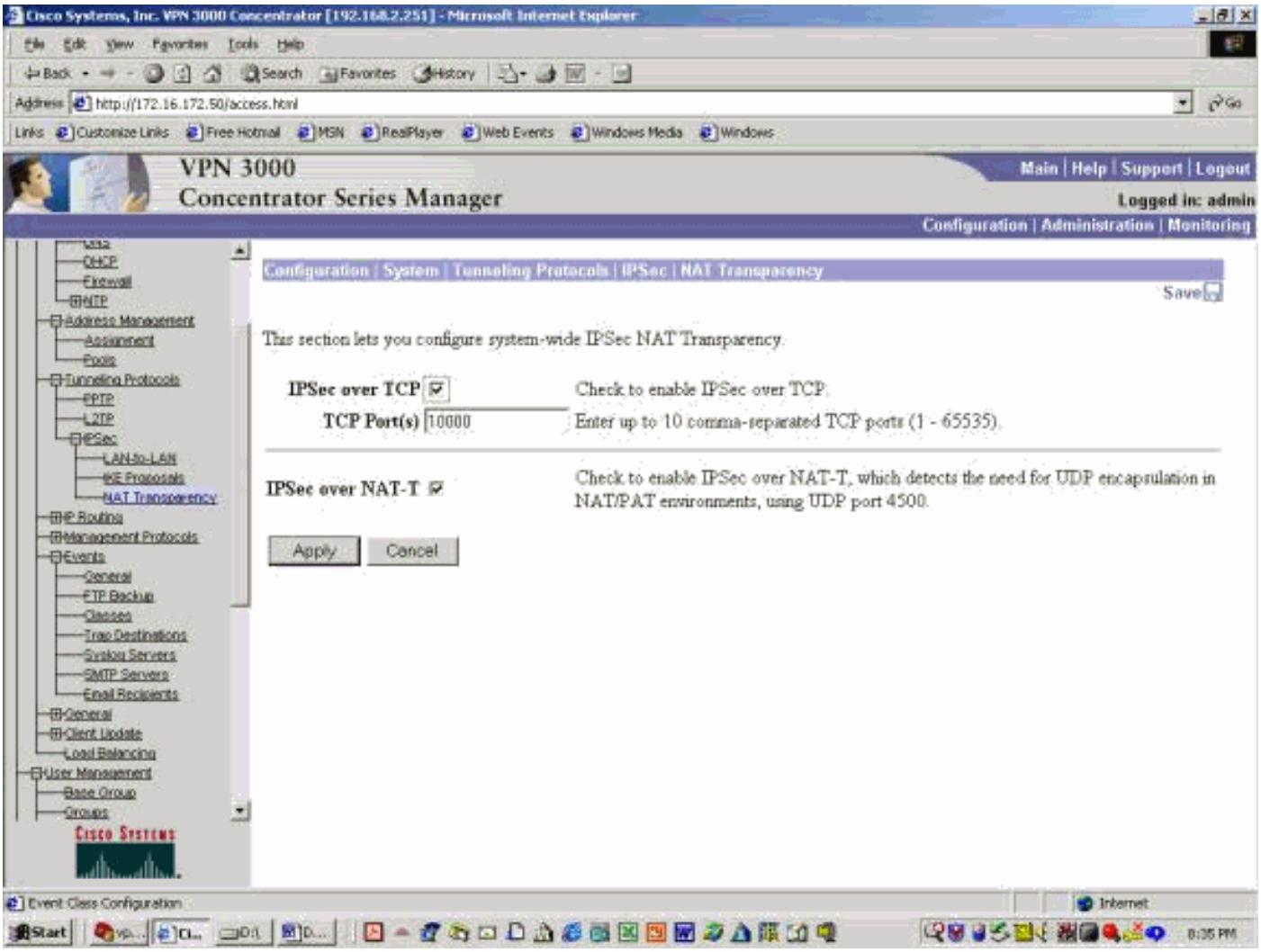
## Configurez le concentrateur VPN 3000

Cette configuration d'échantillon suppose que le concentrateur VPN 3000 a été déjà configuré pour la connectivité IP, et que des connexions VPN (non-NAT-T) standard ont été déjà établies.

Pour activer NAT-T sur une version de concentrateur VPN 3000 plus tôt que la version 4.1, choisissez les **configurations > le système > les protocoles > l'IPSec de Tunnellisation > transparence NAT**, puis vérifiez l'**IPSec au-dessus de** l'option **NAT-T** sur le concentrateur suivant les indications de l'exemple ci-dessous. L'option NAT-T est éteinte par défaut.

Pour activer NAT-T sur une version 4.1 et ultérieures de concentrateur VPN, naviguez vers la même fenêtre NAT de transparence en choisissant la **configuration > le Tunnellisation et la**

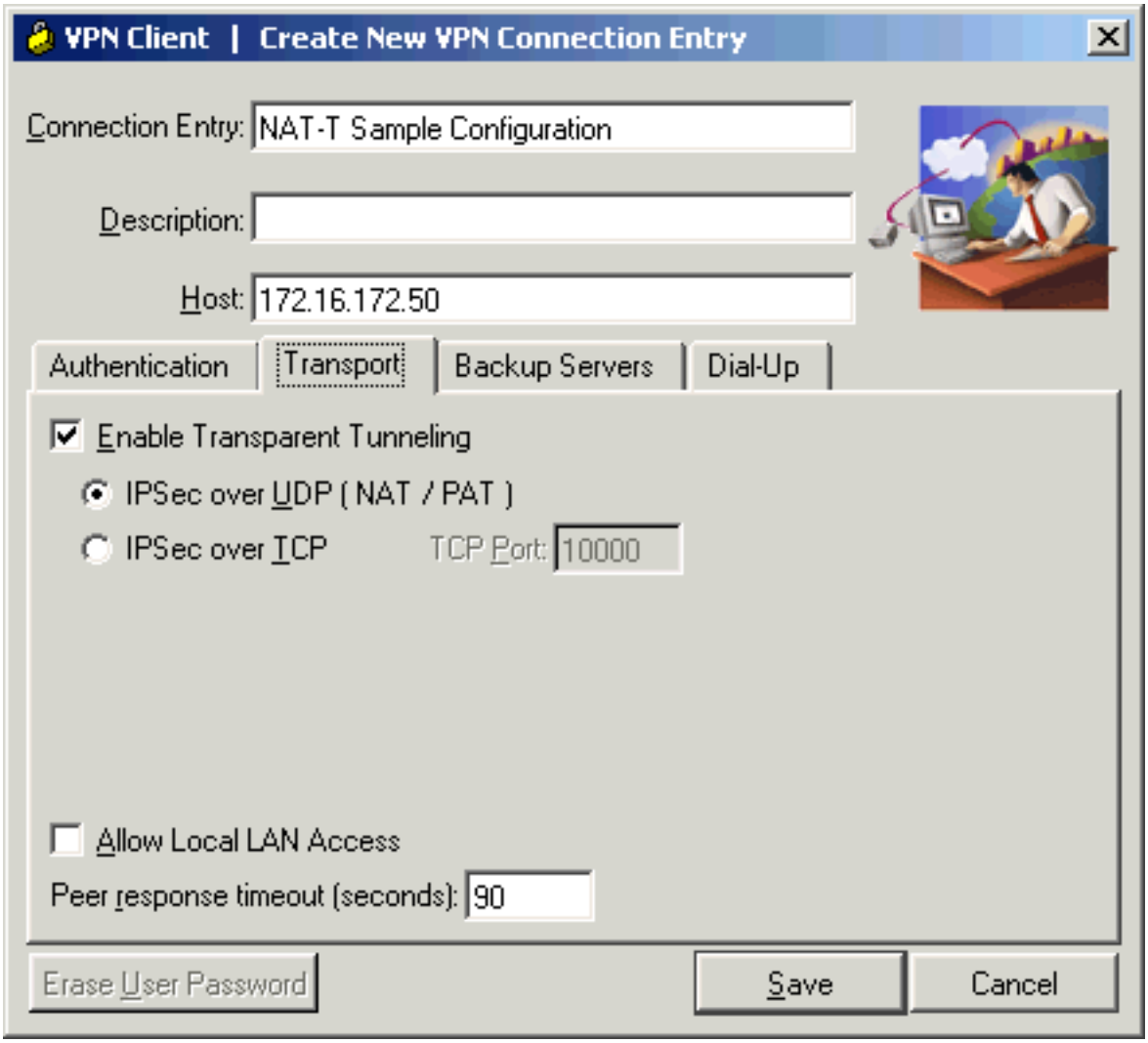
**Sécurité > l'IPSec > transparence NAT.**




## Configurer le client VPN

Pour utiliser NAT-T, **Tunnellisation transparent d'enable de** contrôle. L'exemple suivant explique ceci sur un client VPN plus tard que la version 4.0.

**Remarque:** La même option de configuration est disponible sur la version du client 3.x VPN.




# Vérifiez

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

L'information de dépannage supplémentaire peut être trouvée au dépannage de sécurité IP - comprenant et utilisant des commandes de débogage.

## Vérifiez la configuration PIX

Ces commandes sont utilisées de vérifier la configuration PIX :

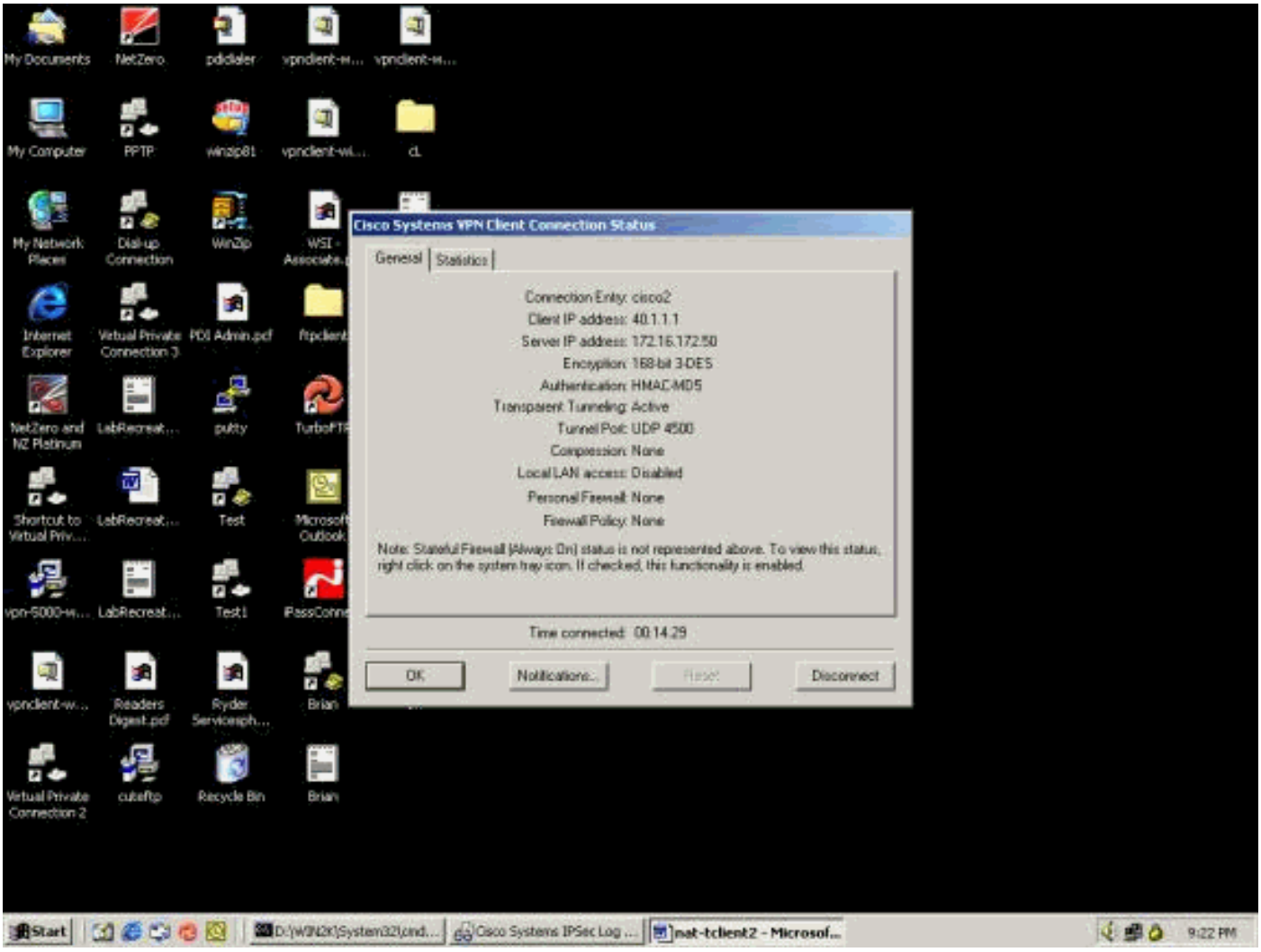
- **show xlate** — Suivant les indications de la sortie ci-dessous, le PIX utilise différents ports de source pour les deux clients vpn, mais les destinations port sont identiques. Tous les paquets de données d'IPSec sont enveloppés utilisant le port UDP 4500. Les négociations de nouvelle saisie ultérieures utilisent également la mêmes source et destinations port.`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** — Utilisez cette commande d'afficher la table de Protocole ARP (Address

Resolution Protocol) et de déterminer si des demandes d'ARP sont traitées.

```
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)#
```

## Statistiques de client vpn

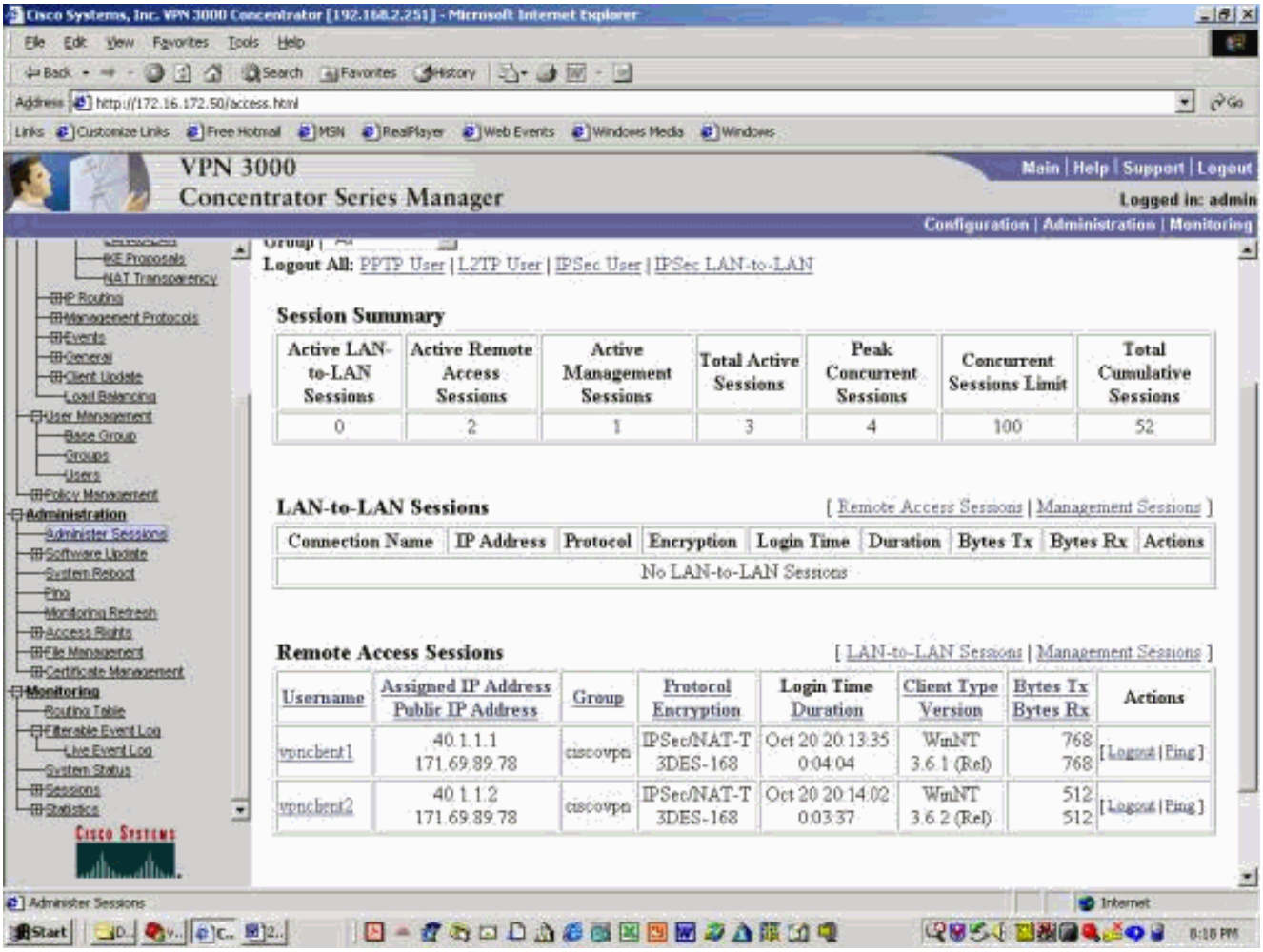
Une fois que le tunnel VPN est établi, cliquez avec le bouton droit sur le verrouillage jaune et choisissez l'**état**. Une fenêtre semblable est affichée ci-dessous. Notez que le port de tunnel est l'UDP 4500, qui montre que vous utilisez NAT-T.



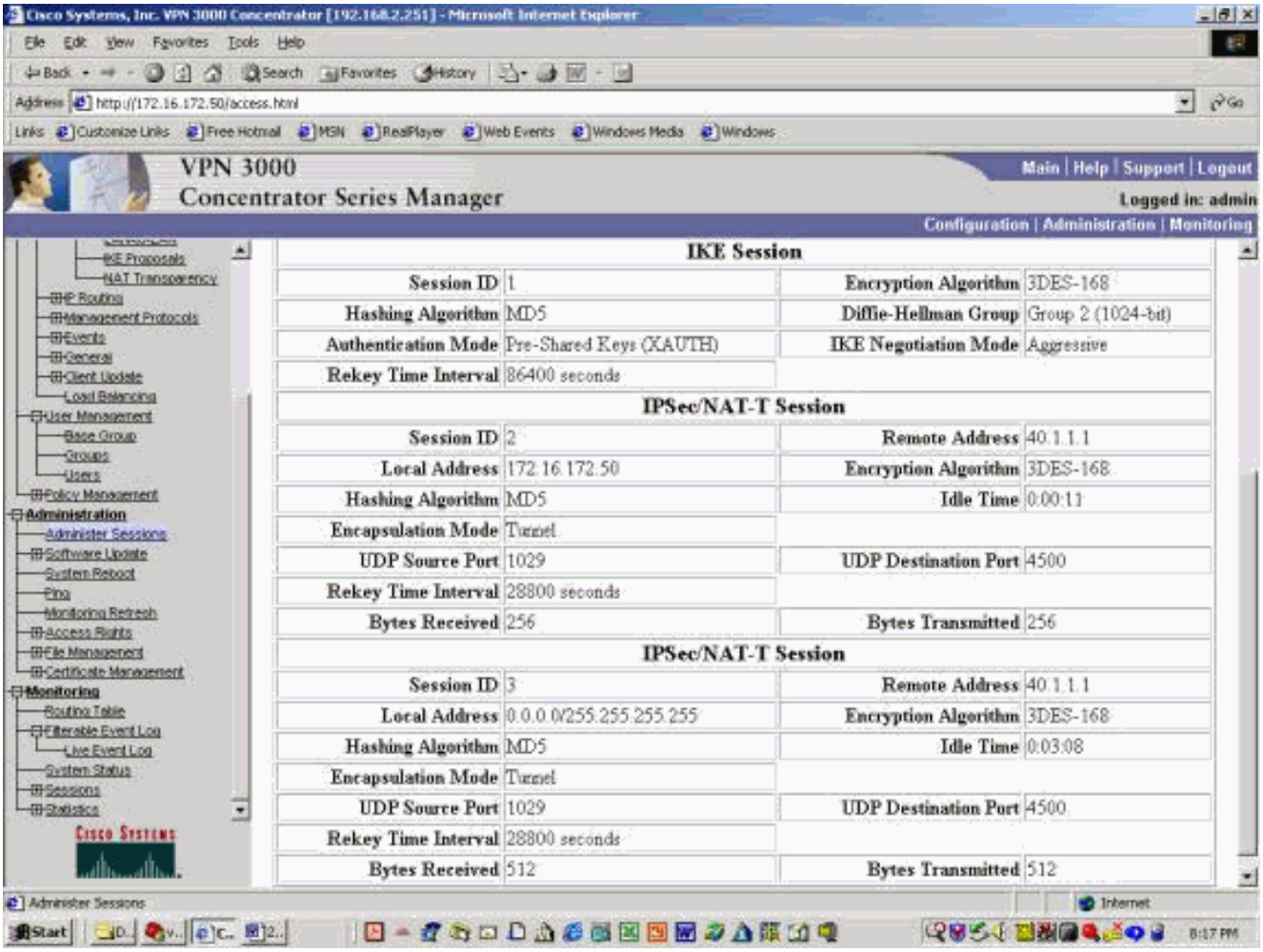

## Statistiques de concentrateur VPN

Procédez comme suit :

1. Sur le concentrateur VPN, choisissez la **gestion > la session d'administrateur**.La session de client vpn peut être vue sous des sessions d'Accès à distance. L'exemple ci-dessous affiche les sessions des deux clients après qu'ils aient établi un tunnel d'IPSec au concentrateur VPN. Ils sont tous deux utilisant l'adresse IP publique 171.69.89.78 et ont été assignés 40.1.1.1 et 40.1.1.2,
   respectivement.




2. Double clic sur un nom d'utilisateur de client.Les statistiques IPSec/IKE sont affichées, comme vu dans l'exemple ci-dessous. Le port de source d'UDP utilisé par le client est 1029, et la destination port utilisée est
4500.




# Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

**Remarque:** Avant d'émettre des commandes de **débogage**, référez-vous aux informations importantes sur des commandes de debug.

**Remarque:** L'information de dépannage supplémentaire PIX peut être trouvée au dépannage de sécurité IP - comprenant et utilisant des commandes de débogage.

## Logs de client vpn

Sur le PC sur lequel le client vpn est installé, ouvrez le visualiseur de log avant d'établir une connexion au concentrateur VPN. Cette sortie de log met en valeur les messages de Nat-T-particularité :

```
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

## Logs de concentrateur VPN

Pour visualiser les logins le concentrateur VPN, choisissent la **surveillance > le journal d'événements filtrables**, et sélectionnent l'**IKE de classes d'événement, l'IKEDBG, l'IKEDECODE**, et l'**IPSECDBG** avec Severities 1 à 13.

```
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

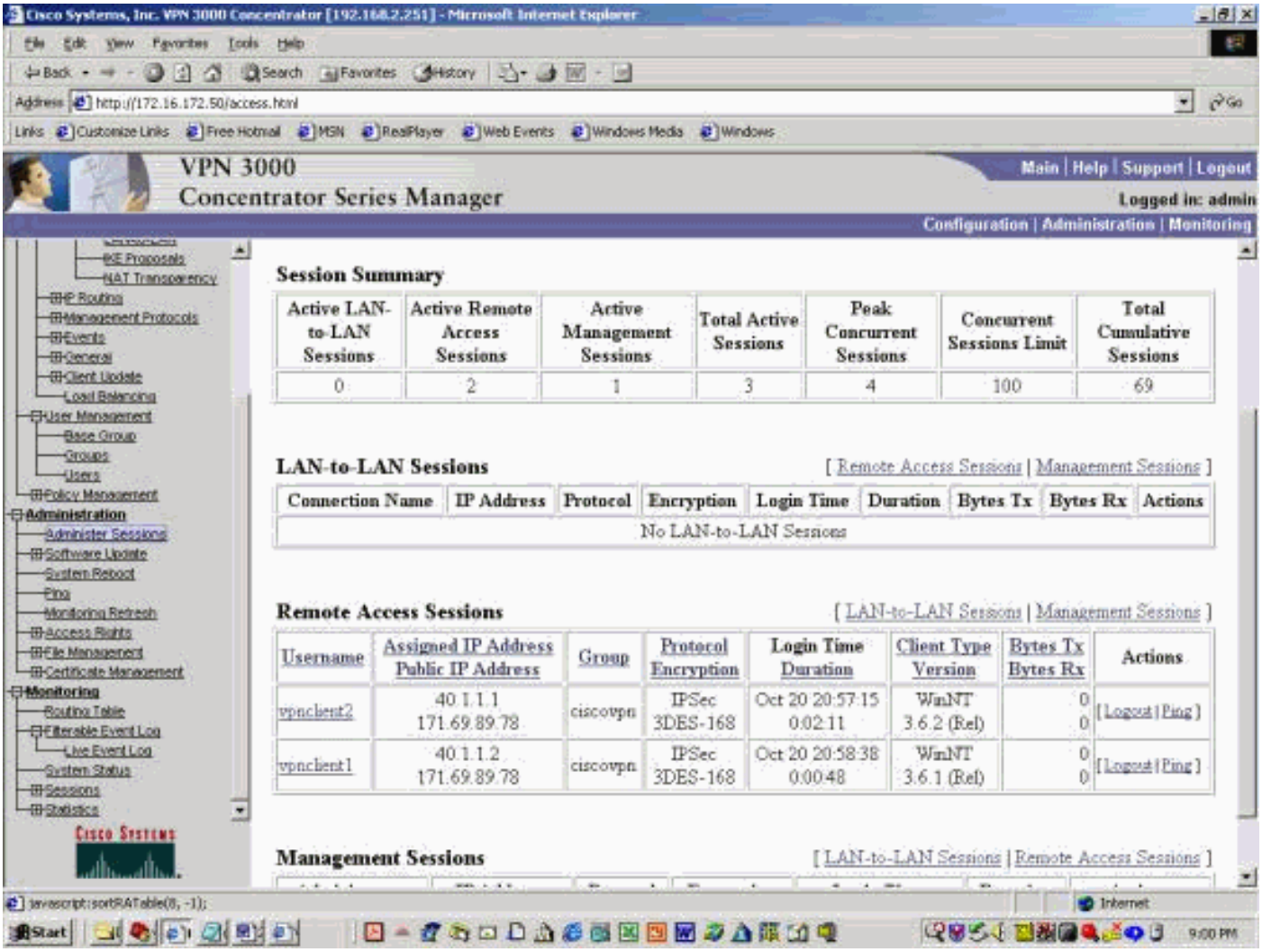
IKEDECODE/0 RPT=8199 171.69.89.78 Notify Payload Decode : DOI : IPSEC (1) Protocol : ISAKMP (1) Message : Altiga keep-alive (40500) Spi : B6 92 24 F4 96 0A 2D 9E 76 FE F6 55 1F 9D 49 F3 Length : 28 3016 10/20/2002 20:23:18.330 SEV=9 IKEDBG/41 RPT=338 171.69.89.78 Group [ciscovpn] User [vpnclient1] Received 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
```

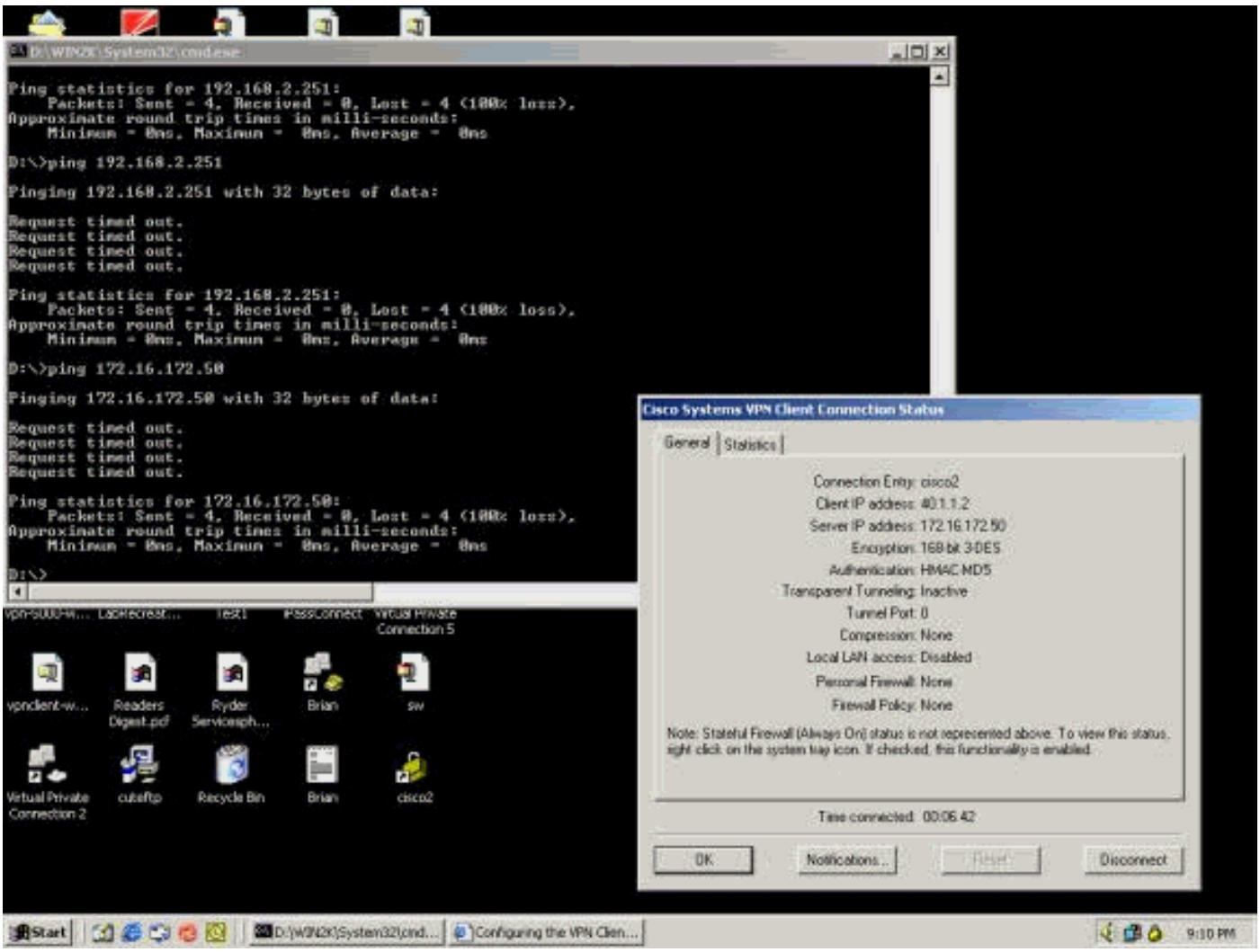
## Dépannage supplémentaire

NAT-T encapsule le trafic d'IPSec dans les datagrammes UDP utilisant le port 4500. Si NAT-T n'est pas vérifié le concentrateur VPN ou si NAT la transparence n'est pas vérifiée le client vpn, le tunnel d'IPSec est établi ; cependant, vous ne pouvez pas ne passer aucune donnée. Pour que NAT-T fonctionne, vous devez avoir le NAT-T vérifié le concentrateur et la transparence NAT (au-dessus de l'UDP) vérifiés le client.

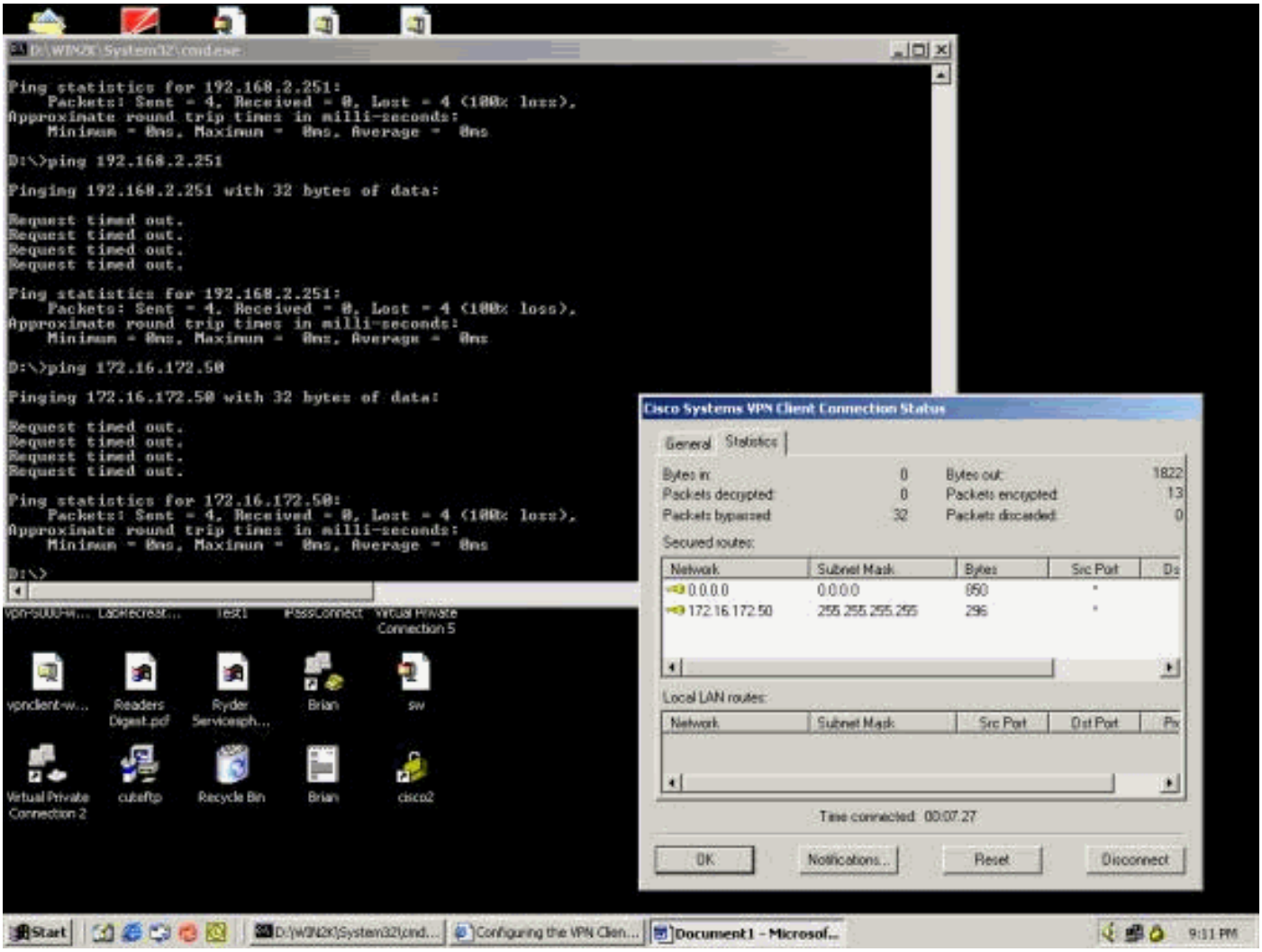
L'exemple ci-dessous affiche un tel cas en lequel NAT-T n'a pas été vérifié le concentrateur. Sur le client, le Tunnellisation transparent a été vérifié. Dans ce cas, un tunnel d'IPSec est établi entre le client et le concentrateur. Cependant puisque les négociations de port de tunnel d'IPSec ont manqué, donnée ne passe pas entre le client et le concentrateur. En soi, les octets transmis et reçus sont zéro pour les sessions d'Accès à distance.



L'exemple ci-dessous affiche les statistiques du client vpn. Notez que le port de tunnel négocié est 0. Il y a une tentative de cingler 192.168.2.251 (interface privée du concentrateur VPN 3000) et 172.16.172.50 d'une invite DOS. Cependant, ces pings manquent parce qu'aucun port de tunnel n'a été négocié et, ainsi, les données d'IPSec sont jetées sur le serveur VPN distant.




L'exemple ci-dessous prouve que le client vpn envoie des données cryptées (13 paquets). Mais le nombre de paquets déchiffrés est zéro pour le serveur VPN distant, et il n'a renvoyé aucune données cryptées. Puisqu'aucun port de tunnel n'a été négocié, le serveur VPN distant jette les paquets et n'envoie aucune donnée de réponse.




# Informations connexes

- Page d'assistance des concentrateurs VPN Cisco 3000
- Page d'assistance du Client VPN 3000 Series Cisco
- Page d'assistance IPsec
- Support et documentation techniques - Cisco Systems