

# Configuration d'un tunnel IPSec entre un client VPN Cisco pour Linux et un concentrateur VPN 3000

## Contenu

[Introduction](#)

[Avant de commencer](#)

[Conventions](#)

[Conditions préalables](#)

[Components Used](#)

[Diagramme du réseau](#)

[Configurations](#)

[Tâche](#)

[Configuration du concentrateur VPN 3000](#)

[Configuration du client Linux](#)

[Vérification](#)

[Dépannage](#)

[Activation de la connexion au client VPN](#)

[Activation de la connexion sur le concentrateur VPN 3000](#)

[Bons débogages](#)

[Causes de problèmes potentiels](#)

[Informations connexes](#)

## [Introduction](#)

Ce document décrit comment former un tunnel IPSec d'un PC Linux exécutant le client VPN Cisco vers un concentrateur Cisco VPN 3000 afin que vous puissiez accéder au réseau à l'intérieur du concentrateur en toute sécurité.

## [Avant de commencer](#)

### [Conventions](#)

Pour plus d'informations sur les conventions des documents, référez-vous aux [Conventions utilisées pour les conseils techniques de Cisco](#).

### [Conditions préalables](#)

Ce document utilise les configurations suivantes :

- [Configuration du concentrateur VPN 3000](#)
- [Configuration du client Linux](#)

## Components Used

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

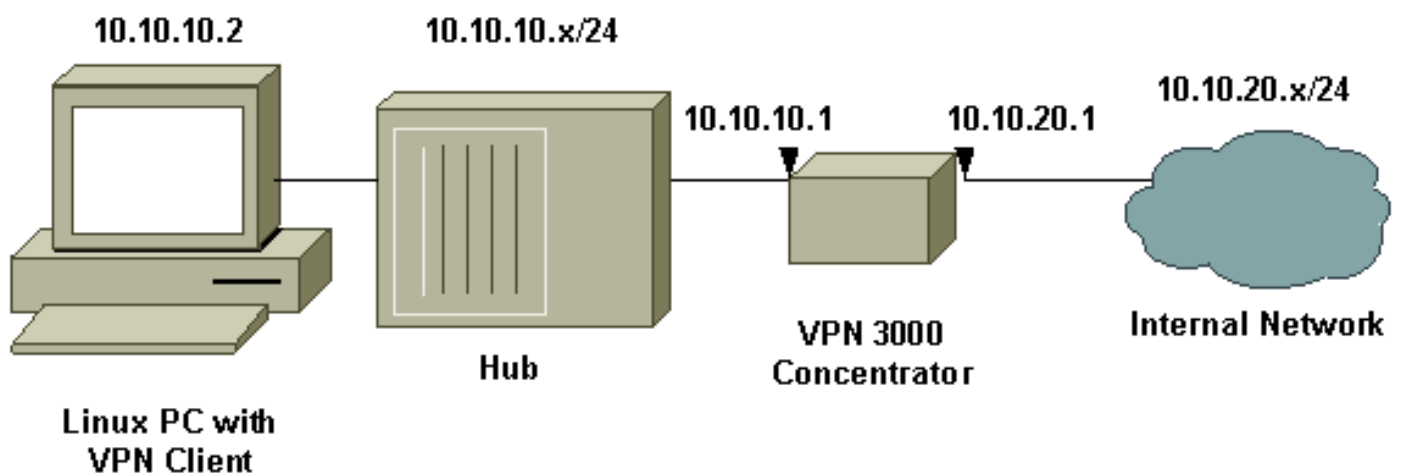
- Concentrateur VPN Cisco 3000 version 3.x
- Client VPN Cisco Version 3.0.8
- Red Hat Linux® version 7.2 avec noyau 2.4.7-10

**Remarque** : la prise en charge de RedHat8 est disponible dans les versions 3.6.2a et ultérieures du client VPN. Les clients enregistrés peuvent obtenir des informations spécifiques en recherchant l'ID de bogue [CSCdy49082](#) (clients [enregistrés](#) uniquement).

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

## Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant :



## Configurations

### Tâche

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

### Configuration du concentrateur VPN 3000

Procédez comme suit pour configurer le concentrateur VPN 3000.

1. Connectez-vous au port de console du concentrateur VPN et vérifiez que des adresses IP

sont attribuées aux interfaces privées (internes) et publiques (externes). Vérifiez également qu'une passerelle par défaut est attribuée afin que le concentrateur puisse transférer les paquets pour les destinations qu'il ne connaît pas à la passerelle par défaut. **Remarque** : La valeur par défaut est normalement le routeur de passerelle Internet.

- 1) Configuration
- 2) Administration
- 3) Monitoring
- 4) Save changes to Config file
- 5) Help Information
- 6) Exit

Main -> 1

- 1) Interface Configuration
- 2) System Management
- 3) User Management
- 4) Policy Management
- 5) Back

Config -> 1

**Ce tableau présente les adresses IP actuelles.**

Interface	IP Address/Subnet Mask	MAC Address
Ethernet 1 - Private	10.10.20.1/255.255.255.0	00.90.A4.00.16.54
Ethernet 2 - Public	10.10.10.1/255.255.255.0	00.90.A4.00.16.55
Ethernet 3 - External	0.0.0.0/0.0.0.0	

- 1) Configure Ethernet #1 (Private)
- 2) Configure Ethernet #2 (Public)
- 3) Configure Ethernet #3 (External)
- 4) Configure Power Supplies
- 5) Configure Expansion Cards
- 6) Back

Interfaces -> 6

- 1) Interface Configuration
- 2) System Management
- 3) User Management
- 4) Policy Management
- 5) Back

Config -> 2

- 1) Servers (Authentication, Accounting, etc.)
- 2) Address Management
- 3) Tunneling Protocols (PPTP, L2TP, etc.)
- 4) IP Routing (static routes, OSPF, etc.)
- 5) Management Protocols (Telnet, TFTP, FTP, etc.)
- 6) Event Configuration
- 7) General Config (system name, time, etc.)
- 8) Back

System -> 4

- 1) Static Routes
- 2) Default Gateways
- 3) OSPF
- 4) OSPF Areas
- 5) DHCP
- 6) Redundancy

7) Back

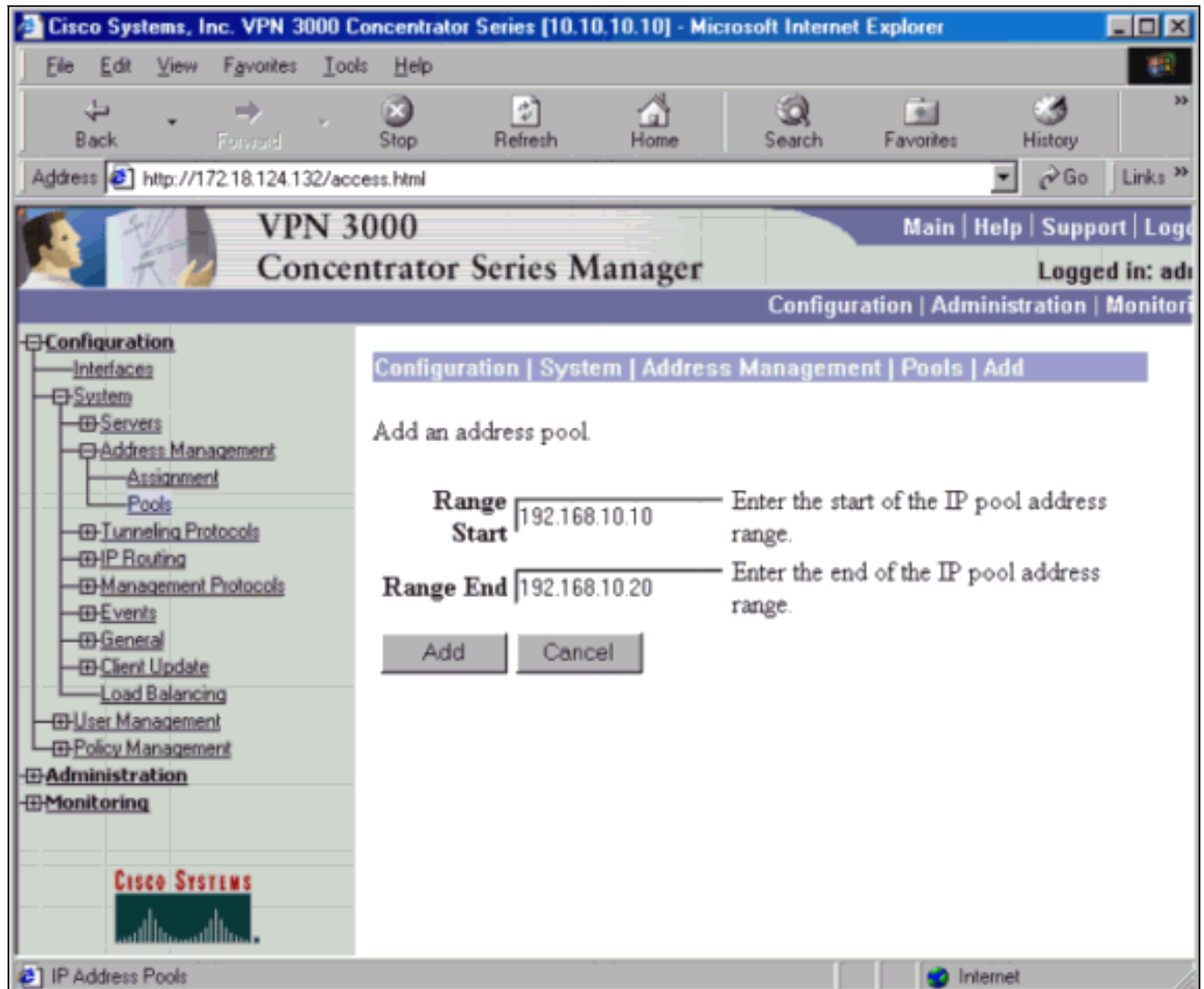
Routing -> 1

Static Routes

Destination	Mask	Metric	Destination
0.0.0.0	0.0.0.0	1	10.10.10.1

- 1) Add Static Route
- 2) Modify Static Route
- 3) Delete Static Route
- 4) Back

2. Pour attribuer une plage d'adresses IP disponible, pointez un navigateur sur l'interface interne du concentrateur VPN 3000 et accédez à **Configuration > System > Address Management > Pools > Add**. Spécifiez une plage d'adresses IP qui ne sont en conflit avec aucun autre périphérique du réseau interne.



3. Pour indiquer au concentrateur VPN d'utiliser le pool, accédez à **Configuration > System > Address Management > Assignment**, puis cochez la case **Use Address Pools**.

4. Configurez un groupe IPsec pour les utilisateurs en accédant à **Configuration > User Management > Groups > Add** et en définissant un nom de groupe et un mot de passe. L'exemple ci-dessous utilise le nom de groupe « ipsecgroup » avec le mot de passe/verify comme « cisco123.

»

Cisco Systems, Inc. VPN 3000 Concentrator Series [10.10.10.10] - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History

Address http://172.18.124.132/access.html Go Links

VPN 3000 Concentrator Series Manager Main Help Support Log

Logged in: ad

Configuration Administration Monitor

Configuration

- Interfaces
- System
  - Servers
  - Address Management
    - Assignment
    - Pools
  - Tunneling Protocols
  - IP Routing
  - Management Protocols
  - Events
  - General
  - Client Update
  - Load Balancing
- User Management
  - Base Group
  - Groups
  - Users
- Policy Management

Administration

CISCO SYSTEMS

you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity General IPsec PPTP/L2TP

**Identity Parameters**

Attribute	Value	Description
Group Name	ipsecgroup	Enter a unique name for the group.
Password	*****	Enter the password for the group.
Verify	*****	Verify the group's password.
Type	Internal	<i>External groups</i> are configured on an external authentication server (e.g. RADIUS). <i>Internal groups</i> are configured on the VPN 3000 Concentrator Series's Internal Database.

Add Cancel

User/Group Management Internet

- Dans l'onglet Groupes généraux, sélectionnez IPsec.

Cisco Systems, Inc. VPN 3000 Concentrator Series [10.10.10.10] - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History

Address http://172.18.124.132/access.html Go Links

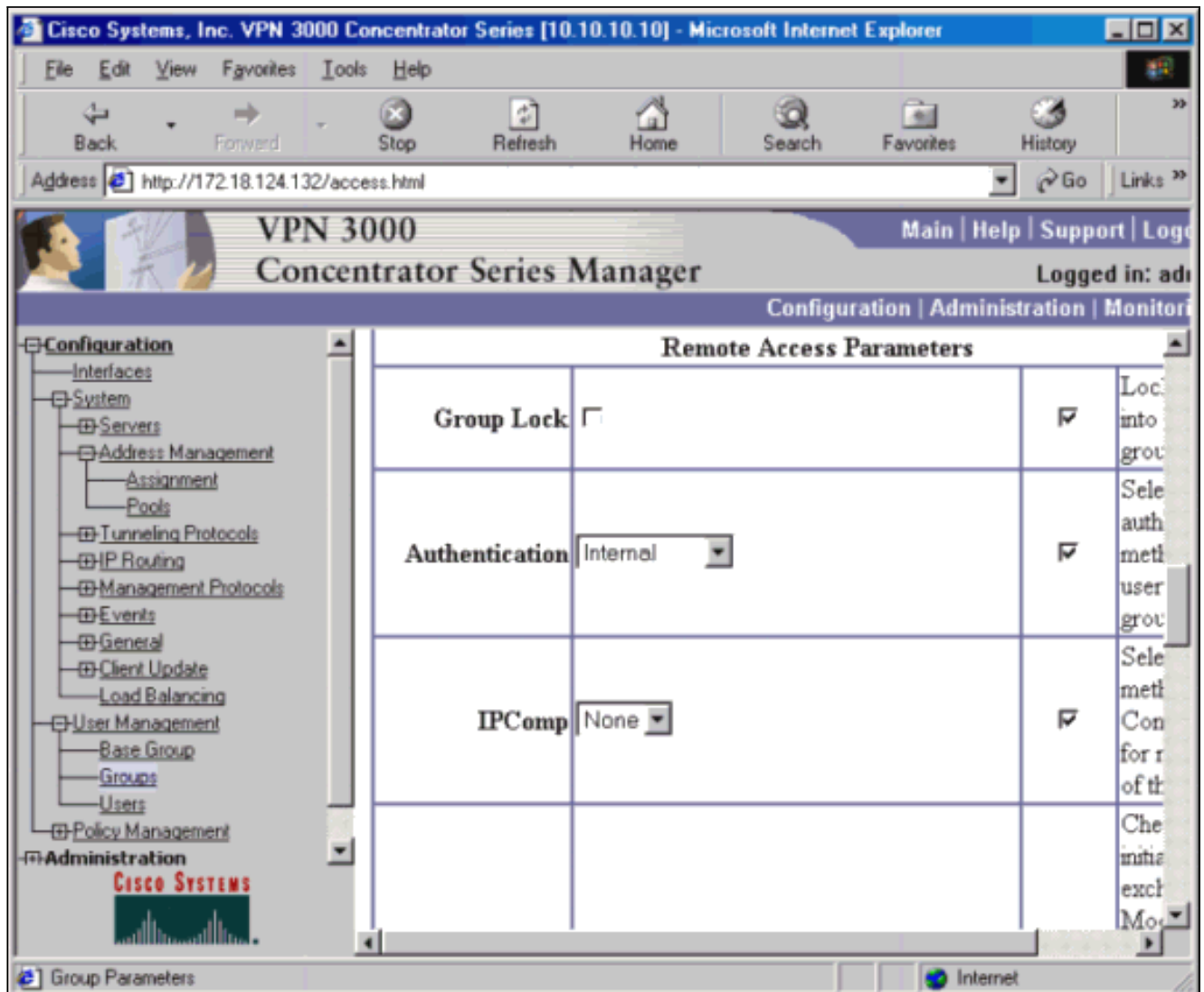
**VPN 3000 Concentrator Series Manager** Main | Help | Support | Logg  
 Logged in: ad

Configuration | Administration | Monitor

<b>Configuration</b>				server.
Interfaces				
System				
Servers				
Address Management				
Assignment				
Pools				
Tunneling Protocols				
IP Routing				
Management Protocols				
Events				
General				
Client Update				
Load Balancing				
User Management				
Base Group				
Groups				
Users				
Policy Management				
Administration				
<b>CISCO SYSTEMS</b>				
	<b>Primary WINS</b>	<input type="text"/>	<input checked="" type="checkbox"/>	Enter the IP address of the primary WINS server.
	<b>Secondary WINS</b>	<input type="text"/>	<input checked="" type="checkbox"/>	Enter the IP address of the secondary WINS server.
	<b>SEP Card Assignment</b>	<input checked="" type="checkbox"/> SEP 1 <input checked="" type="checkbox"/> SEP 2 <input checked="" type="checkbox"/> SEP 3 <input checked="" type="checkbox"/> SEP 4	<input checked="" type="checkbox"/>	Select the SEP cards this group can be assigned to.
	<b>Tunneling Protocols</b>	<input type="checkbox"/> PPTP <input type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPsec <input type="checkbox"/> L2TP over IPsec	<input type="checkbox"/>	Select the tunneling protocols this group can connect with.
	<b>Strip Realm</b>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to remove the realm qualifier of the user name during authentication.

Group Parameters Internet

6. Dans l'onglet Groupes IPsec, définissez l'authentification sur Interne.



7. Accédez à **Configuration > User Management > Users > Add**, puis ajoutez un utilisateur au groupe précédemment défini. Dans l'exemple ci-dessous, l'utilisateur est « ipsecuser » avec le mot de passe « xyz12345 » dans le groupe « ipsecgroup ».



**Identity Parameters**

Attribute	Value	Description
User Name	ipsecuser	Enter a unique user name.
Password	XXXXXXXXXX	Enter the user's password. The password must satisfy the group password requirements.
Verify	XXXXXXXXXX	Verify the user's password
Group	ipsecgroup	Enter the group to which this user belongs.
IP Address		Enter the IP address assigned to this user.
Subnet Mask		Enter the subnet mask assigned to this user.

Add Cancel

## [Configuration du client Linux](#)

Suivez ces étapes :

1. Accédez au répertoire `/etc/CiscoSystemsVPNlient/Profiles` dans lequel les profils de connexion VPN sont stockés.

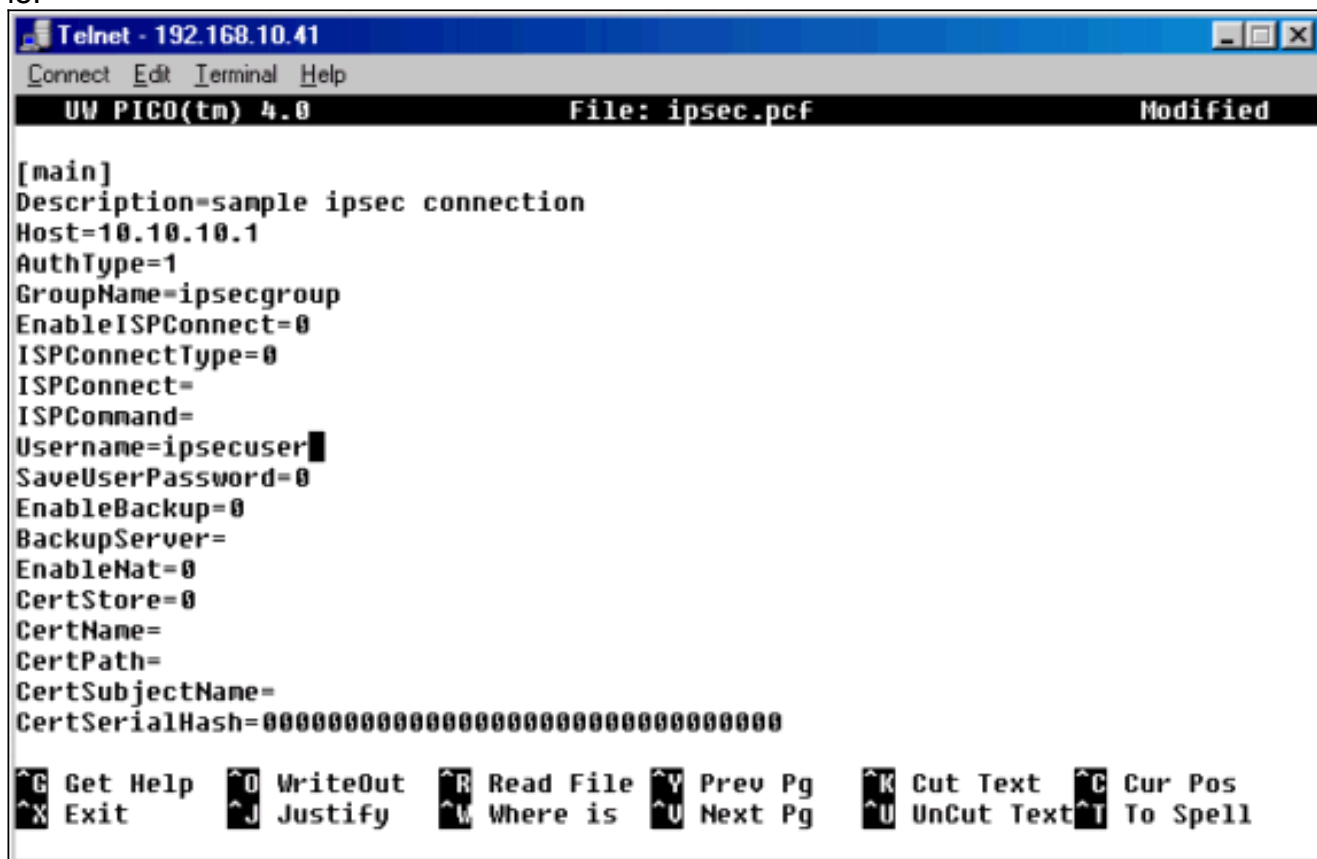
```
Telnet - 192.168.10.41
Connect Edit Terminal Help
Red Hat Linux release 7.2 (Enigma)
Kernel 2.4.7-10 on an i686
login: jbiersba
Password:
Last login: Mon Nov  5 12:46:38 from 192.168.10.42
[jbiersba@dhcppc1 jbiersba]$ su
Password:
[root@dhcppc1 jbiersba]# cd /etc/CiscoSystemsUPNClient/
[root@dhcppc1 CiscoSystemsUPNClient]# ls
Certificates Profiles vpnclient.ini
[root@dhcppc1 CiscoSystemsUPNClient]# cd /etc/CiscoSystemsUPNClient/Profiles
[root@dhcppc1 Profiles]# ls
sample.pcf
[root@dhcppc1 Profiles]#
```

2. Ouvrez un nouveau fichier de profil en copiant l'exemple de profil sur un nouveau nom ou en en créant un à partir de zéro. Dans l'exemple ci-dessous, l'exemple de fichier .pcf a été copié, renommé et modifié.

```
Telnet - 192.168.10.41
Connect Edit Terminal Help
Red Hat Linux release 7.2 (Enigma)
Kernel 2.4.7-10 on an i686
login: jbiersba
Password:
Last login: Mon Nov  5 12:46:38 from 192.168.10.42
[jbiersba@dhcppc1 jbiersba]$ su
Password:
[root@dhcppc1 jbiersba]# cd /etc/CiscoSystemsUPNClient/
[root@dhcppc1 CiscoSystemsUPNClient]# ls
Certificates Profiles vpnclient.ini
[root@dhcppc1 CiscoSystemsUPNClient]# cd /etc/CiscoSystemsUPNClient/Profiles
[root@dhcppc1 Profiles]# ls
sample.pcf
[root@dhcppc1 Profiles]# cp sample.pcf ipsec.pcf
[root@dhcppc1 Profiles]# ls
ipsec.pcf sample.pcf
[root@dhcppc1 Profiles]#
```

3. Modifiez le nouveau fichier .pcf pour inclure les informations suivantes. Une nouvelle description qui identifie la connexion Une nouvelle adresse IP d'hôte qui sera l'adresse IP de l'interface publique du concentrateur VPN 3000 Un nouveau nom de groupe qui devra

correspondre au groupe configuré dans la configuration du groupe VPN 3000 Nouveau nom d'utilisateur qui est le même nom d'utilisateur configuré sur le concentrateur VPN 3000 qui coïncide avec le groupe VPN sur le concentrateur Enregistrez le fichier et quittez-le.

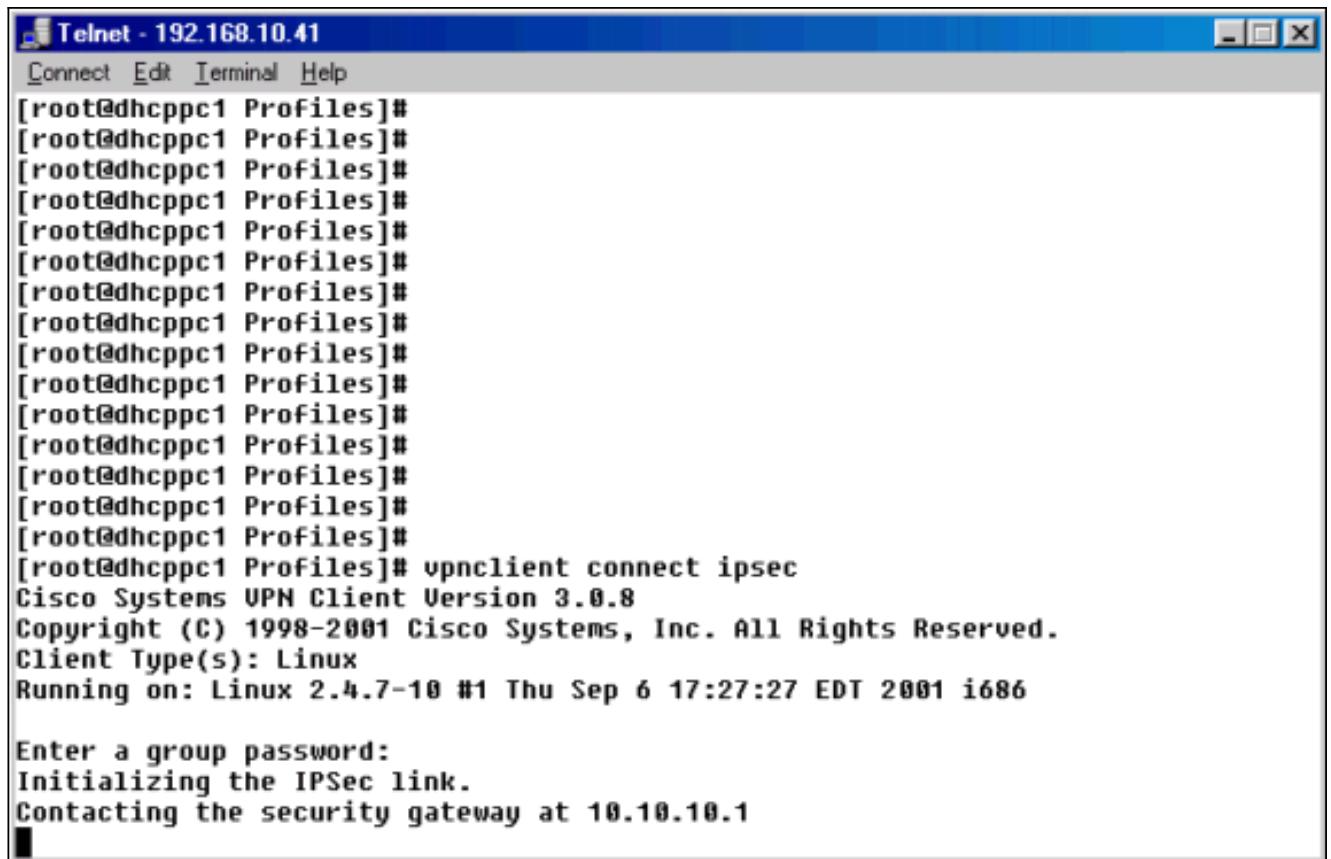


```
Telnet - 192.168.10.41
Connect Edit Terminal Help
UW PICO(tm) 4.0 File: ipsec.pcf Modified

[main]
Description=sample ipsec connection
Host=10.10.10.1
AuthType=1
GroupName=ipsecgroup
EnableISPConnect=0
ISPConnectType=0
ISPConnect=
ISPCommand=
Username=ipsecuser
SaveUserPassword=0
EnableBackup=0
BackupServer=
EnableNat=0
CertStore=0
CertName=
CertPath=
CertSubjectName=
CertSerialHash=000000000000000000000000000000000000

^G Get Help ^O WriteOut ^R Read File ^V Prev Pg ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where is ^U Next Pg ^U UnCut Text ^I To Spell
```

4. À partir de l'invite de commandes, utilisez la commande **vpnclient connect ipsec** pour vous connecter au concentrateur VPN à l'aide du fichier IPsec .pcf. Vous serez invité à saisir le mot de passe du groupe. Il s'agit du même mot de passe qui a été configuré sur le concentrateur VPN 3000 (mot de passe « xyz12345 », dans cet exemple).



```
Telnet - 192.168.10.41
Connect Edit Terminal Help
[root@dhcppc1 Profiles]#
[root@dhcppc1 Profiles]#
[root@dhcppc1 Profiles]#
[root@dhcppc1 Profiles]#
[root@dhcppc1 Profiles]#
[root@dhcppc1 Profiles]#
[root@dhcppc1 Profiles]#
[root@dhcppc1 Profiles]#
[root@dhcppc1 Profiles]#
[root@dhcppc1 Profiles]#
[root@dhcppc1 Profiles]#
[root@dhcppc1 Profiles]#
[root@dhcppc1 Profiles]#
[root@dhcppc1 Profiles]#
[root@dhcppc1 Profiles]#
[root@dhcppc1 Profiles]#
[root@dhcppc1 Profiles]#
[root@dhcppc1 Profiles]# upnclient connect ipsec
Cisco Systems UPN Client Version 3.0.8
Copyright (C) 1998-2001 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Linux
Running on: Linux 2.4.7-10 #1 Thu Sep 6 17:27:27 EDT 2001 i686

Enter a group password:
Initializing the IPsec link.
Contacting the security gateway at 10.10.10.1
```

5. Si la connexion échoue, reportez-vous à la section [Dépannage](#) ci-dessous.

## [Vérification](#)

Aucune procédure de vérification n'est disponible pour cette configuration.

## [Dépannage](#)

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

### [Activation de la connexion au client VPN](#)

Voici les informations de dépannage concernant cette configuration. Suivez les instructions ci-dessous pour dépanner votre configuration.

1. Créez un profil global, s'il n'en existe pas déjà dans le répertoire /etc/CiscoSystemsVPNClient/. Le profil global devrait ressembler à l'exemple ci-dessous.

```
Telnet - 192.168.10.41
Connect Edit Terminal Help
UW PICO(tm) 4.0 File: vpnclient.ini

[main]
BinDirPath=/usr/local/bin
RunAtLogon=0
EnableLog=1
[LOG.IKE]
LogLevel=3
[LOG.CH]
LogLevel=3
[LOG.PPP]
LogLevel=3
[LOG.DIALER]
LogLevel=3
[LOG.CUPND]
LogLevel=3
[LOG.CERT]
LogLevel=3
[LOG.IPSEC]
LogLevel=3
[CertEnrollment]

^G Get Help ^O WriteOut ^R Read File ^V Prev Pg ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where is ^U Next Pg ^U UnCut Text ^T To Spell
```

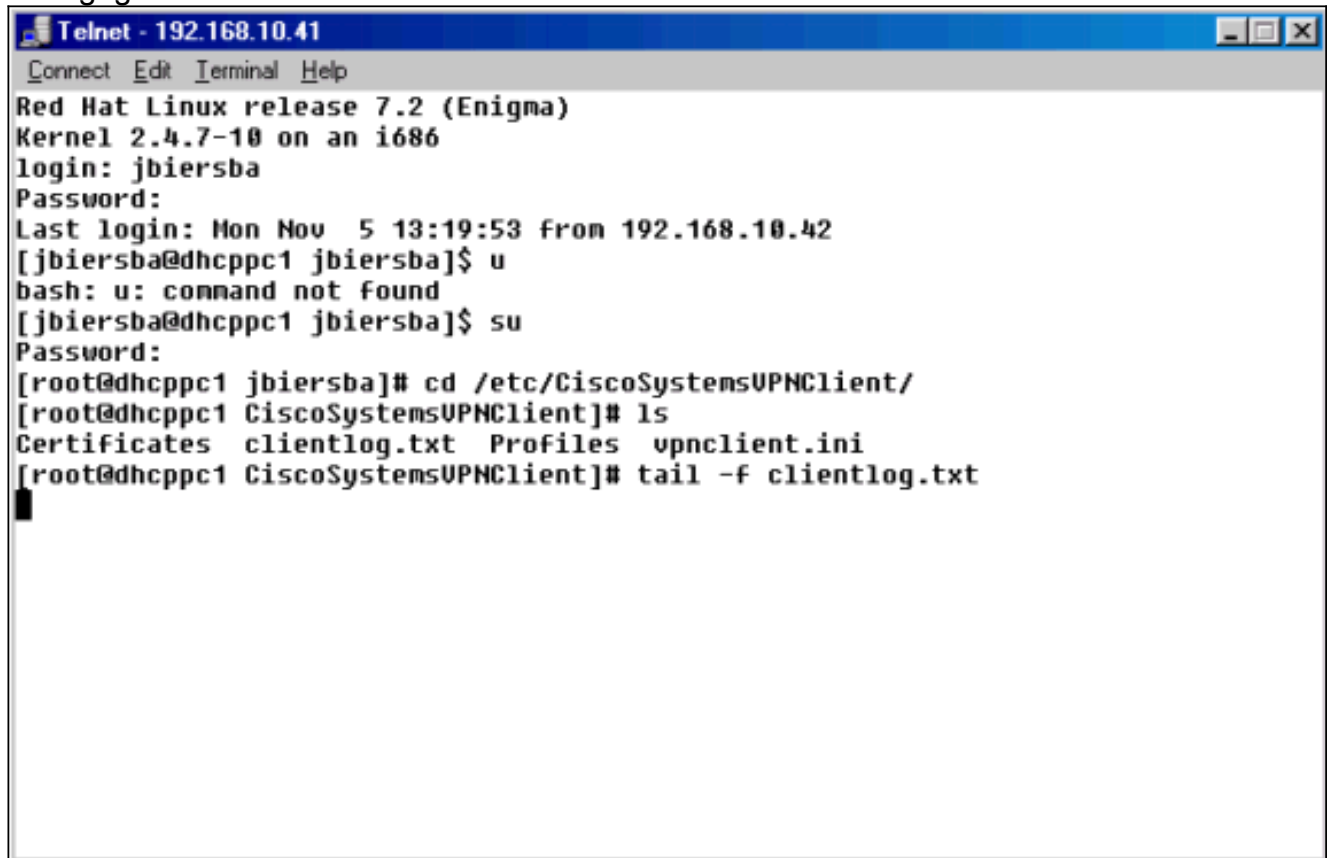
**Remarque :** vérifiez que chacun des niveaux de journal est défini sur 3 ; cela permettra d'atteindre le plus haut niveau de journalisation possible.

2. À partir de l'invite de commandes, utilisez la commande `/usr/local/bin/ipseclog` pour démarrer l'utilitaire de journalisation IPsec et déplacer les informations de ce journal vers un répertoire et un fichier de votre choix. Dans cet exemple, le fichier porte le nom `clientlog.txt` et se trouve dans le répertoire `/etc/CiscoSystemsVPNClient`

```
Telnet - 192.168.10.41
Connect Edit Terminal Help
[LOG.DIALER]
LogLevel=3
[LOG.CUPND]
LogLevel=3
[LOG.CERT]
LogLevel=3
[LOG.IPSEC]
LogLevel=3
[CertEnrollment]

[root@dhcpc1 CiscoSystemsUPNClient]# /usr/local/bin/ipseclog /etc/CiscoSystemsU
PNClient/clientlog.txt
bash: /usr/local/bin/ipseclog: No such file or directory
[root@dhcpc1 CiscoSystemsUPNClient]# ./usr/local/bin/ipseclog /etc/CiscoSystem
sUPNClient/clientlog.txt
bash: ./usr/local/bin/ipseclog: No such file or directory
[root@dhcpc1 CiscoSystemsUPNClient]# /usr/local/bin/ipseclog /etc/CiscoSystems
UPNClient/clientlog.txt
Cisco Systems UPN Client Version 3.0.8
Copyright (C) 1998-2001 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Linux
Running on: Linux 2.4.7-10 #1 Thu Sep 6 17:27:27 EDT 2001 i686
```

3. Dans une fenêtre séparée, utilisez la commande **tail -f** (pour nom de fichier) pour obtenir un instantané mis à jour en permanence du fichier clientlog.txt pendant que vous vous connectez pour recueillir des informations de débogage.



```
Telnet - 192.168.10.41
Connect Edit Terminal Help
Red Hat Linux release 7.2 (Enigma)
Kernel 2.4.7-10 on an i686
login: jbiersba
Password:
Last login: Mon Nov  5 13:19:53 from 192.168.10.42
[jbiersba@dhcpcpc1 jbiersba]$ u
bash: u: command not found
[jbiersba@dhcpcpc1 jbiersba]$ su
Password:
[root@dhcpcpc1 jbiersba]# cd /etc/CiscoSystemsUPNClient/
[root@dhcpcpc1 CiscoSystemsUPNClient]# ls
Certificates clientlog.txt Profiles vpnclient.ini
[root@dhcpcpc1 CiscoSystemsUPNClient]# tail -f clientlog.txt
```

## [Activation de la connexion sur le concentrateur VPN 3000](#)

Suivez les instructions ci-dessous pour dépanner votre configuration.

1. Accédez à **Configuration > System > Events > Classes** pour activer le débogage suivant en cas d'échec de connexion d'événement.AUTH - Gravité du journal 1-13AUTHDBG - Gravité du journal 1-13IKE - Gravité du journal 1-13IKEDBG - Gravité du journal 1-13IPSEC - Gravité du journal 1-13IPSECDBG - Gravité du journal 1-13**Remarque** : Si nécessaire, AUTHDECODE, IKEDECODE et IPSECDECODE peuvent être ajoutés ultérieurement.

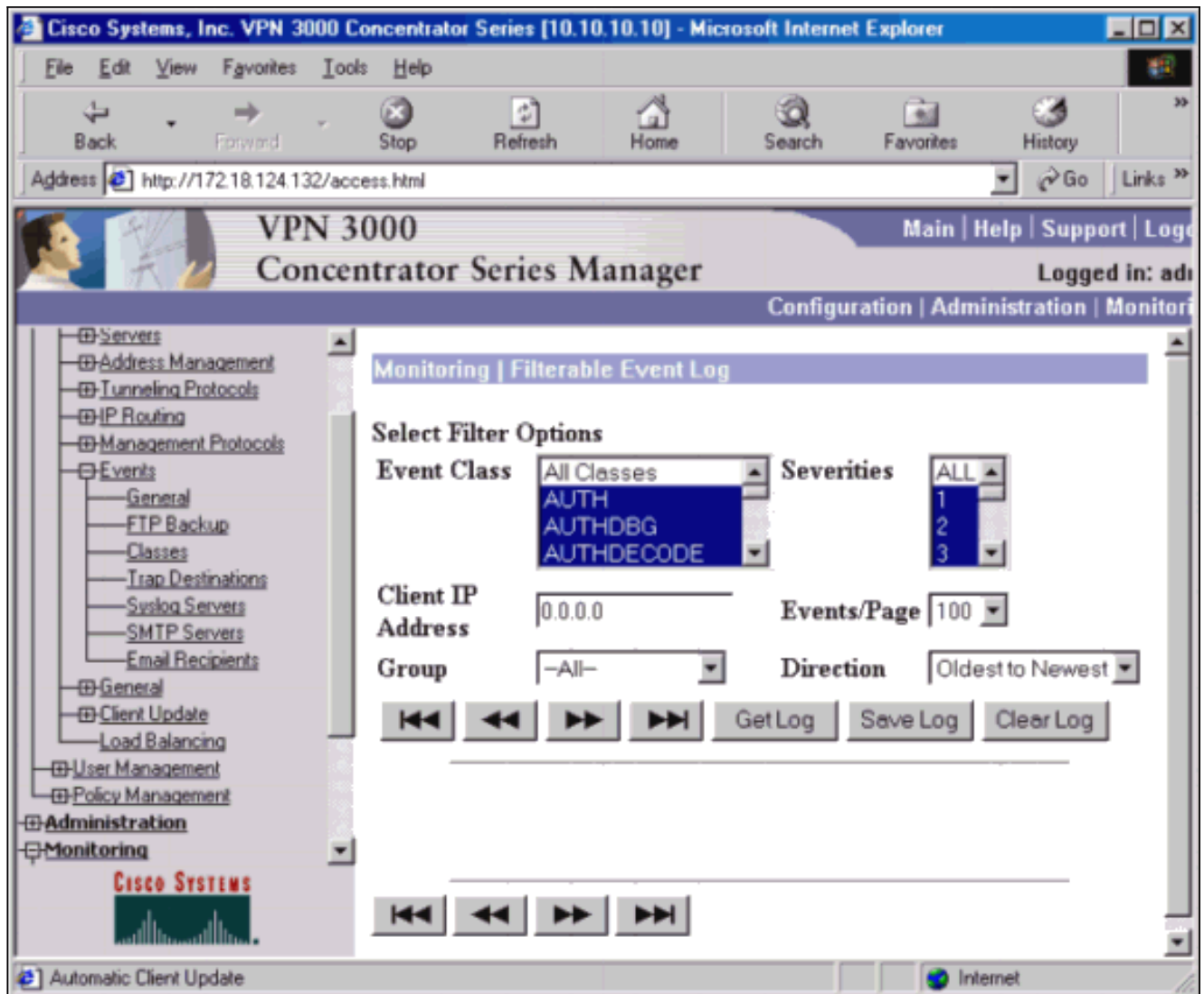
This section lets you configure special handling of specific event classes.

Click the **Add** button to add an event class, or select an event class and click **Modify** or **Delete**.

[Click here to configure general event parameters.](#)

Configured Event Classes	Actions
AUTH	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>
AUTHDBG	
IKE	
IKEDBG	
IPSEC	
IPSECDBG	

2. Vous pouvez afficher le journal en accédant à **Monitoring > Filterable Event Log**.



## Bons débogages

- [Client VPN](#)
- [Concentrateur VPN 3000](#)

### Client VPN

```
1 14:02:24.118 11/05/2001 Sev=Info/4 CVPND/0x4340000F
```

Started cvpnd:

Cisco Systems VPN Client Version 3.0.8

Copyright (C) 1998-2001 Cisco Systems, Inc. All Rights Reserved.

Client Type(s): Linux

Running on: Linux 2.4.7-10 #1 Thu Sep 6 17:27:27 EDT 2001 i686

```
2 14:02:24.118 11/05/2001 Sev=Info/4 IPSEC/0x43700013
```

Delete internal key with SPI=0xcfa58e9f

```
3 14:02:24.118 11/05/2001 Sev=Info/4 IPSEC/0x4370000C
```



Key deleted by SPI 0xcfa58e9f

4 14:02:24.118 11/05/2001 Sev=Info/4 IPSEC/0x43700013

Delete internal key with SPI=0x3a21bb45

5 14:02:24.118 11/05/2001 Sev=Info/4 IPSEC/0x4370000C

Key deleted by SPI 0x3a21bb45

6 14:02:24.118 11/05/2001 Sev=Info/4 IPSEC/0x43700013

Delete internal key with SPI=0xc76d7f87

7 14:02:24.118 11/05/2001 Sev=Info/4 IPSEC/0x4370000C

Key deleted by SPI 0xc76d7f87

8 14:02:24.118 11/05/2001 Sev=Info/4 IPSEC/0x43700013

Delete internal key with SPI=0x8fd46a6a

9 14:02:24.118 11/05/2001 Sev=Info/4 IPSEC/0x4370000C

Key deleted by SPI 0x8fd46a6a

10 14:02:24.119 11/05/2001 Sev=Info/4 IPSEC/0x43700014

Deleted all keys

11 14:02:24.119 11/05/2001 Sev=Info/4 IPSEC/0x43700014

Deleted all keys

12 14:02:24.119 11/05/2001 Sev=Info/4 IPSEC/0x4370000A

IPSec driver successfully stopped

13 14:02:24.119 11/05/2001 Sev=Info/4 IPSEC/0x43700014

Deleted all keys

14 14:02:24.119 11/05/2001 Sev=Info/4 IPSEC/0x43700008

IPSec driver successfully started

15 14:02:24.119 11/05/2001 Sev=Info/4 IPSEC/0x43700014

Deleted all keys

16 14:02:24.119 11/05/2001 Sev=Info/4 IPSEC/0x4370000D

Key(s) deleted by Interface (192.168.10.41)

17 14:02:24.960 11/05/2001 Sev=Info/4 CM/0x43100002

Begin connection process

18 14:02:24.963 11/05/2001 Sev=Info/4 CM/0x43100004

Establish secure connection using Ethernet

19 14:02:24.963 11/05/2001 Sev=Info/4 CM/0x43100026

Attempt connection with server "rtp-vpn-cluster.cisco.com"

20 14:02:24.980 11/05/2001 Sev=Info/6 IKE/0x4300003B

Attempting to establish a connection with 161.44.127.194.

21 14:02:25.136 11/05/2001 Sev=Debug/7 IKE/0x4300000A

Sending ID me = ID\_KEY ciscovpncluster-nat.

22 14:02:25.136 11/05/2001 Sev=Info/4 IKE/0x43000013

SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID) to 161.44.127.194

23 14:02:25.139 11/05/2001 Sev=Decode/11 IKE/0x43000001

ISAKMP Header

Initiator COOKIE: ACD9BE3AC57BBE35

Responder COOKIE: 0000000000000000

Next Payload: Security Association

Ver: 10

Exchange Type: Aggressive Mode

Flags: (none)

MessageID: 00000000

Length: 469762048

Payload Security Association

Next Payload: Key Exchange

Reserved: 0000

Payload Length: 308

DOI: IPsec

Situation:(SIT\_IDENTITY\_ONLY)

Payload Proposal

Next Payload: None

Reserved: 0000

Payload Length: 296

Proposal #: 1

Protocol-Id: PROTO\_ISAKMP

SPI Size: 0

# of transforms: 8

SPI:

Payload Transform

Next Payload: Transform

Reserved: 0000

Payload Length: 36

Transform #: 1

Transform-Id: KEY\_IKE

Reserved2: 0000

Encryption Algorithm: 3DES-CBC

Hash Algorithm: SHA1

Group Description: Group 2

Authentication Method: XAUTHInitPreShared

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Transform

Next Payload: Transform

Reserved: 0000

Payload Length: 36

Transform #: 2

Transform-Id: KEY\_IKE

Reserved2: 0000

Encryption Algorithm: 3DES-CBC

Hash Algorithm: MD5

Group Description: Group 2

Authentication Method: XAUTHInitPreShared

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Transform

Next Payload: Transform

Reserved: 0000

Payload Length: 36

Transform #: 3

Transform-Id: KEY\_IKE

Reserved2: 0000

Encryption Algorithm: 3DES-CBC

Hash Algorithm: SHA1

Group Description: Group 2

Authentication Method: Preshared key

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Transform

Next Payload: Transform

Reserved: 0000

Payload Length: 36

Transform #: 4

Transform-Id: KEY\_IKE

Reserved2: 0000

Encryption Algorithm: 3DES-CBC

Hash Algorithm: MD5

Group Description: Group 2

Authentication Method: Preshared key

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Transform

Next Payload: Transform

Reserved: 0000

Payload Length: 36

Transform #: 5

Transform-Id: KEY\_IKE

Reserved2: 0000

Encryption Algorithm: DES-CBC

Hash Algorithm: SHA1

Group Description: Group 2

Authentication Method: XAUTHInitPreShared

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Transform

Next Payload: Transform

Reserved: 0000

Payload Length: 36

Transform #: 6

Transform-Id: KEY\_IKE

Reserved2: 0000

Encryption Algorithm: DES-CBC

Hash Algorithm: MD5

Group Description: Group 2

Authentication Method: XAUTHInitPreShared

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Transform

Next Payload: Transform

Reserved: 0000

Payload Length: 36

Transform #: 7

Transform-Id: KEY\_IKE

Reserved2: 0000

Encryption Algorithm: DES-CBC

Hash Algorithm: SHA1

Group Description: Group 2

Authentication Method: Preshared key

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 36

Transform #: 8

Transform-Id: KEY\_IKE

Reserved2: 0000

Encryption Algorithm: DES-CBC

Hash Algorithm: MD5

Group Description: Group 2

Authentication Method: Preshared key

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Key Exchange

Next Payload: Nonce

Reserved: 0000

Payload Length: 132

Data: 14B9E06FB0742252C9CDA9C0E1045036FCE13E88E84A868EE895743  
287DBD865FF938F144197B85865F39D6ED5BF7B16CBE49EA64DF07CE6840D  
4105D800CE463CB310BF85D145CF63659CD9F7403CF486C27C37D086A4A57  
5AE655F547DF9FF1DAC0F5ECE37FA5D91DC58F3B1C3331D78C6D711C316A1  
70A8515219147FB0C405000018

Payload Nonce

Next Payload: Identification

Reserved: 0000

Payload Length: 24

Data: 18ADE217264969EBC698E5742FDAE5A6F1E8555F0D00001B

Payload Identification

Next Payload: Vendor ID

Reserved: 0000

Payload Length: 27

ID Type: ID\_KEY\_ID

Protocol ID (UDP/TCP, etc...): 17

Port: 500

ID Data: ciscovpncluster-nat

Payload Vendor ID

Next Payload: Vendor ID

Reserved: 0000

Payload Length: 12

Data (In Hex): 09002689DFD6B712

Payload Vendor ID

Next Payload: Vendor ID

Reserved: 0000

Payload Length: 20

Data (In Hex): AFCAD71368A1F1C96B8696FC77570100

Payload Vendor ID

Next Payload: None

Reserved: 0000

Payload Length: 20

Data (In Hex): 12F5F28C457168A9702D9FE274CC0100

24 14:02:25.140 11/05/2001 Sev=Info/4 IPSEC/0x43700014

Deleted all keys

25 14:02:25.140 11/05/2001 Sev=Info/4 IPSEC/0x4370000D

Key(s) deleted by Interface (192.168.10.41)

26 14:02:25.341 11/05/2001 Sev=Info/5 IKE/0x4300002F

Received ISAKMP packet: peer = 161.44.127.194

27 14:02:25.343 11/05/2001 Sev=Decode/11 IKE/0x43000001

ISAKMP Header

Initiator COOKIE: ACD9BE3AC57BBE35

Responder COOKIE: F8D106BDD3A6236D

Next Payload: Security Association

Ver: 10

Exchange Type: Aggressive Mode

Flags: (none)

MessageID: 00000000

Length: 344

Payload Security Association

Next Payload: Key Exchange

Reserved: 0000

Payload Length: 56

DOI: IPsec

Situation: (SIT\_IDENTITY\_ONLY)

Payload Proposal

Next Payload: None

Reserved: 0000

Payload Length: 44

Proposal #: 1

Protocol-Id: PROTO\_ISAKMP

SPI Size: 0

# of transforms: 1

SPI:

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 36

Transform #: 2

Transform-Id: KEY\_IKE

Reserved2: 0000

Encryption Algorithm: 3DES-CBC

Hash Algorithm: MD5

Group Description: Group 2

Authentication Method: XAUTHInitPreShared

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Key Exchange

Next Payload: Nonce

Reserved: 0000

Payload Length: 132

Data: 0F428F30FAD939D04BB301934BD24252585691E9A5AA30DF3  
E67B04A2BAF010C5B0F890D422AD68592AA11F0AD8DCA20766AF42C  
F93850EC73526CFE91B953CF6A5B38A051CB6D7673A6F69E15ACE9D  
7793FFC2A89B88135EA5DE187961E64869787008EFCBE1BEF40C34F  
AE1A278F1BEE8DF3BA873DCDA9A33DC14FBE59D77605000018

Payload Nonce



Next Payload: Identification

Reserved: 0000

Payload Length: 24

Data: B466B5297839DDB8D45177EE87DABC1463EB8D4C0800000C

Payload Identification

Next Payload: Hash

Reserved: 0000

Payload Length: 12

ID Type: IPv4 Address

Protocol ID (UDP/TCP, etc...): 17

Port: 500

ID Data: 161.44.127.194

Payload Hash

Next Payload: Vendor ID

Reserved: 0000

Payload Length: 20

Data: E1F2B6C63282B7091A0DA4F1F9C056E30D000014

Payload Vendor ID

Next Payload: Vendor ID

Reserved: 0000

Payload Length: 20

Data (In Hex): 12F5F28C457168A9702D9FE274CC0100

Payload Vendor ID

Next Payload: Vendor ID

Reserved: 0000

Payload Length: 12

Data (In Hex): 09002689DFD6B712

Payload Vendor ID

Next Payload: Vendor ID

Reserved: 0000

Payload Length: 20

Data (In Hex): AFCAD71368A1F1C96B8696FC77570100

Payload Vendor ID

Next Payload: None

Reserved: 0000

Payload Length: 20

Data (In Hex): 1F07F70EAA6514D3B0FA96542A500300

28 14:02:25.344 11/05/2001 Sev=Info/4 IKE/0x43000014

RECEIVING <<< ISAKMP OAK AG (SA, KE, NON, ID, HASH, VID,  
VID, VID, VID) from 161.44.127.194

29 14:02:25.344 11/05/2001 Sev=Info/5 IKE/0x43000059

Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100

30 14:02:25.344 11/05/2001 Sev=Info/5 IKE/0x43000001

Peer is a Cisco-Unity compliant peer

31 14:02:25.344 11/05/2001 Sev=Info/5 IKE/0x43000059

Vendor ID payload = 09002689DFD6B712

32 14:02:25.344 11/05/2001 Sev=Info/5 IKE/0x43000059

Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100

33 14:02:25.344 11/05/2001 Sev=Info/5 IKE/0x43000001

Peer supports DPD

34 14:02:25.344 11/05/2001 Sev=Info/5 IKE/0x43000059

Vendor ID payload = 1F07F70EAA6514D3B0FA96542A500300

35 14:02:25.480 11/05/2001 Sev=Info/4 IKE/0x43000013

SENDING >>> ISAKMP OAK AG \*(HASH, NOTIFY:STATUS\_INITIAL\_CONTACT)  
to 161.44.127.194

36 14:02:25.483 11/05/2001 Sev=Decode/11 IKE/0x43000001

ISAKMP Header

Initiator COOKIE: ACD9BE3AC57BBE35

Responder COOKIE: F8D106BDD3A6236D

Next Payload: Hash

Ver: 10

Exchange Type: Aggressive Mode

Flags: (Encryption)

MessageID: 00000000

Length: 469762048

Payload Hash

Next Payload: Notification

Reserved: 0000

Payload Length: 20

Data: CFCFC21977456B8B6BA6D39AB4EB14B20000001C

Payload Notification

Next Payload: None

Reserved: 0000

Payload Length: 28

DOI: IPsec

Protocol-ID: PROTO\_ISAKMP

Spi Size: 16

Notify Type: STATUS\_INITIAL\_CONTACT

SPI: ACD9BE3AC57BBE35F8D106BDD3A6236D

Data:

37 14:02:25.524 11/05/2001 Sev=Info/5 IKE/0x4300002F

Received ISAKMP packet: peer = 161.44.127.194

38 14:02:25.524 11/05/2001 Sev=Debug/7 IKE/0x43000022

Crypto READY becoming ACTIVE

39 14:02:25.527 11/05/2001 Sev=Decode/11 IKE/0x43000001

ISAKMP Header

Initiator COOKIE: ACD9BE3AC57BBE35

Responder COOKIE: F8D106BDD3A6236D

Next Payload: Hash

Ver: 10

Exchange Type: Informational

Flags: (Encryption)

MessageID: 9A429435

Length: 84

Payload Hash

Next Payload: Notification

Reserved: 0000

Payload Length: 20

Data: 09ED923D74F93C252C056B96F374E80900000020

Payload Notification

Next Payload: None

Reserved: 0000

Payload Length: 32

DOI: IPsec

Protocol-ID: PROTO\_ISAKMP

Spi Size: 16

Notify Type: NOTIFY\_STATUS\_LOAD\_BALANCE

SPI: ACD9BE3AC57BBE35F8D106BDD3A6236D

Data: A12C7FC4

40 14:02:25.527 11/05/2001 Sev=Info/4 IKE/0x43000014

RECEIVING <<< ISAKMP OAK INFO \*(HASH, NOTIFY:LOAD\_BALANCE)  
from 161.44.127.194

41 14:02:25.527 11/05/2001 Sev=Info/4 CM/0x4310001B

Received alternative server address "161.44.127.196" from  
primary server

42 14:02:25.527 11/05/2001 Sev=Debug/8 IKE/0x4300004C

Stopping DPD timer for IKE SA\* 0817FC98

43 14:02:25.528 11/05/2001 Sev=Info/4 IKE/0x43000013

SENDING >>> ISAKMP OAK INFO \*(HASH, DEL) to 161.44.127.194

44 14:02:25.530 11/05/2001 Sev=Decode/11 IKE/0x43000001

ISAKMP Header

Initiator COOKIE: ACD9BE3AC57BBE35

Responder COOKIE: F8D106BDD3A6236D

Next Payload: Hash

Ver: 10

Exchange Type: Informational

Flags: (Encryption)

MessageID: D3B8CE2C

Length: 469762048

Payload Hash

Next Payload: Delete

Reserved: 0000

Payload Length: 20

Data: D1461180C869DA6D6A7BDE0A34CE7D030000001C

Payload Delete

Next Payload: None

Reserved: 0000

Payload Length: 28

DOI: Isakmp

Protocol-ID: PROTO\_ISAKMP

Spi Size: 16

# of SPIs: 1

SPI (Hex dump): ACD9BE3AC57BBE35F8D106BDD3A6236D

45 14:02:25.531 11/05/2001 Sev=Info/4 CM/0x43100014

Unable to establish Phase 1 SA with server  
"rtp-vpn-cluster.cisco.com" because of "DEL\_REASON\_LOAD\_BALANCING"

46 14:02:25.531 11/05/2001 Sev=Info/4 CM/0x43100010

Try alternative server "161.44.127.196" given by the  
primary server

47 14:02:25.531 11/05/2001 Sev=Info/4 CM/0x43100026

Attempt connection with server "161.44.127.196"

48 14:02:25.531 11/05/2001 Sev=Info/6 IKE/0x4300003B

Attempting to establish a connection with 161.44.127.196.

49 14:02:25.678 11/05/2001 Sev=Debug/7 IKE/0x4300000A

Sending ID me = ID\_KEY ciscovpncluster-nat.

50 14:02:25.678 11/05/2001 Sev=Info/4 IKE/0x43000013

SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID)  
to 161.44.127.196

51 14:02:25.681 11/05/2001 Sev=Decode/11 IKE/0x43000001

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 0000000000000000

Next Payload: Security Association

Ver: 10

Exchange Type: Aggressive Mode

Flags: (none)

MessageID: 00000000

Length: 469762048

Payload Security Association

Next Payload: Key Exchange

Reserved: 0000

Payload Length: 308

DOI: IPsec

Situation:(SIT\_IDENTITY\_ONLY)

Payload Proposal

Next Payload: None

Reserved: 0000

Payload Length: 296

Proposal #: 1

Protocol-Id: PROTO\_ISAKMP

SPI Size: 0

# of transforms: 8

SPI:

Payload Transform

Next Payload: Transform

Reserved: 0000

Payload Length: 36

Transform #: 1

Transform-Id: KEY\_IKE

Reserved2: 0000

Encryption Algorithm: 3DES-CBC

Hash Algorithm: SHA1

Group Description: Group 2

Authentication Method: XAUTHInitPreShared

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Transform

Next Payload: Transform

Reserved: 0000

Payload Length: 36

Transform #: 2

Transform-Id: KEY\_IKE

Reserved2: 0000

Encryption Algorithm: 3DES-CBC

Hash Algorithm: MD5

Group Description: Group 2

Authentication Method: XAUTHInitPreShared

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Transform

Next Payload: Transform

Reserved: 0000

Payload Length: 36

Transform #: 3

Transform-Id: KEY\_IKE

Reserved2: 0000

Encryption Algorithm: 3DES-CBC

Hash Algorithm: SHA1

Group Description: Group 2

Authentication Method: Preshared key

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Transform

Next Payload: Transform

Reserved: 0000

Payload Length: 36

Transform #: 4

Transform-Id: KEY\_IKE

Reserved2: 0000

Encryption Algorithm: 3DES-CBC

Hash Algorithm: MD5

Group Description: Group 2

Authentication Method: Preshared key

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Transform

Next Payload: Transform

Reserved: 0000

Payload Length: 36

Transform #: 5

Transform-Id: KEY\_IKE

Reserved2: 0000

Encryption Algorithm: DES-CBC

Hash Algorithm: SHA1

Group Description: Group 2

Authentication Method: XAUTHInitPreShared

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Transform

Next Payload: Transform

Reserved: 0000

Payload Length: 36

Transform #: 6

Transform-Id: KEY\_IKE

Reserved2: 0000



Encryption Algorithm: DES-CBC

Hash Algorithm: MD5

Group Description: Group 2

Authentication Method: XAUTHInitPreShared

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Transform

Next Payload: Transform

Reserved: 0000

Payload Length: 36

Transform #: 7

Transform-Id: KEY\_IKE

Reserved2: 0000

Encryption Algorithm: DES-CBC

Hash Algorithm: SHA1

Group Description: Group 2

Authentication Method: Preshared key

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 36

Transform #: 8

Transform-Id: KEY\_IKE

Reserved2: 0000

Encryption Algorithm: DES-CBC

Hash Algorithm: MD5

Group Description: Group 2

Authentication Method: Preshared key

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Key Exchange

Next Payload: Nonce

Reserved: 0000

Payload Length: 132

Data: 7F445582B28E0DA53D4D7C42E50582503B5771C46C357F98  
4DCB7A9549F5F6789E05016095F4FEFD3C2B1206CBCE63681AF2D5  
5BEED5524D989636C22523665E58F7D338DFD7D7F838CF4A0514C7  
F3F87BECB053E257D08B8A2AD988AABB63B692852FFE4E550C4020  
A0A3058170F6CA53C3C2BEC27045FD8B7C724E2ED1BD3405000018

Payload Nonce

Next Payload: Identification

Reserved: 0000

Payload Length: 24

Data: 5A57FF12D4D74824EB0103E3E2D7C3A5403BDA0F0D00001B

Payload Identification

Next Payload: Vendor ID

Reserved: 0000

Payload Length: 27

ID Type: ID\_KEY\_ID

Protocol ID (UDP/TCP, etc...): 17

Port: 500

ID Data: ciscovpncluster-nat

Payload Vendor ID

Next Payload: Vendor ID

Reserved: 0000

Payload Length: 12

Data (In Hex): 09002689DFD6B712

Payload Vendor ID

Next Payload: Vendor ID

Reserved: 0000

Payload Length: 20

Data (In Hex): AFCAD71368A1F1C96B8696FC77570100

Payload Vendor ID

Next Payload: None

Reserved: 0000

Payload Length: 20

Data (In Hex): 12F5F28C457168A9702D9FE274CC0100

52 14:02:25.682 11/05/2001 Sev=Debug/8 IKE/0x4300004C

Stopping DPD timer for IKE SA\* 0817FC98

53 14:02:25.682 11/05/2001 Sev=Info/5 IKE/0x4300002F

Received ISAKMP packet: peer = 161.44.127.194

54 14:02:25.682 11/05/2001 Sev=Warning/2 IKE/0xC3000080

Received an IKE packet from someone other than the  
Concentrator that we are currently connected to... discarding packet.

55 14:02:25.883 11/05/2001 Sev=Info/5 IKE/0x4300002F

Received ISAKMP packet: peer = 161.44.127.196

56 14:02:25.886 11/05/2001 Sev=Decode/11 IKE/0x43000001

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Security Association

Ver: 10

Exchange Type: Aggressive Mode

Flags: (none)

MessageID: 00000000

Length: 344

Payload Security Association

Next Payload: Key Exchange

Reserved: 0000

Payload Length: 56

DOI: IPsec

Situation:(SIT\_IDENTITY\_ONLY)

Payload Proposal

Next Payload: None

Reserved: 0000

Payload Length: 44

Proposal #: 1

Protocol-Id: PROTO\_ISAKMP

SPI Size: 0

# of transforms: 1

SPI:

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 36

Transform #: 2

Transform-Id: KEY\_IKE

Reserved2: 0000

Encryption Algorithm: 3DES-CBC

Hash Algorithm: MD5

Group Description: Group 2

Authentication Method: XAUTHInitPreShared

Life Type: seconds

Life Duration (Hex): 9BC42000

Payload Key Exchange

Next Payload: Nonce

Reserved: 0000

Payload Length: 132

Data: 71A75D31C3251028E8B893C8268A3CBF626ADCC4BE8A550F  
C2EFFAD981C25B68145B42F554E505CD90C1309F46335EF4E1E064  
9A54C5D1E0496E5A169690B1FAA8AFE69271C09D9189EFE993CBD5  
BECB9FF304F00BA8CD6509551FC7D5BB3AB97FF3464E4E29400232  
88BBF1E698C3E0C58BCAD5D69E881F47981CCA00E221DA05000018

Payload Nonce

Next Payload: Identification

Reserved: 0000

Payload Length: 24

Data: 392387EED0F758D660D57DF42F937AD1EE2A80AF0800000C

Payload Identification

Next Payload: Hash

Reserved: 0000

Payload Length: 12

ID Type: IPv4 Address

Protocol ID (UDP/TCP, etc...): 17

Port: 500

ID Data: 161.44.127.196

Payload Hash

Next Payload: Vendor ID

Reserved: 0000

Payload Length: 20

Data: FD17C6600A11AB661CF746CA2B9BB0CE0D000014

Payload Vendor ID

Next Payload: Vendor ID

Reserved: 0000

Payload Length: 20

Data (In Hex): 12F5F28C457168A9702D9FE274CC0100

Payload Vendor ID

Next Payload: Vendor ID

Reserved: 0000

Payload Length: 12

Data (In Hex): 09002689DFD6B712

Payload Vendor ID

Next Payload: Vendor ID

Reserved: 0000

Payload Length: 20

Data (In Hex): AFCAD71368A1F1C96B8696FC77570100

Payload Vendor ID

Next Payload: None

Reserved: 0000

Payload Length: 20

Data (In Hex): 1F07F70EAA6514D3B0FA96542A500300

57 14:02:25.887 11/05/2001 Sev=Info/4 IKE/0x43000014

RECEIVING <<< ISAKMP OAK AG (SA, KE, NON, ID, HASH, VID,  
VID, VID, VID) from 161.44.127.196

58 14:02:25.887 11/05/2001 Sev=Info/5 IKE/0x43000059

Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100

59 14:02:25.887 11/05/2001 Sev=Info/5 IKE/0x43000001

Peer is a Cisco-Unity compliant peer

60 14:02:25.887 11/05/2001 Sev=Info/5 IKE/0x43000059

Vendor ID payload = 09002689DFD6B712

61 14:02:25.887 11/05/2001 Sev=Info/5 IKE/0x43000059

Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100

62 14:02:25.887 11/05/2001 Sev=Info/5 IKE/0x43000001

Peer supports DPD

63 14:02:25.887 11/05/2001 Sev=Info/5 IKE/0x43000059

Vendor ID payload = 1F07F70EAA6514D3B0FA96542A500300

64 14:02:26.036 11/05/2001 Sev=Info/4 IKE/0x43000013

SENDING >>> ISAKMP OAK AG \*(HASH, NOTIFY:STATUS\_INITIAL\_CONTACT)  
to 161.44.127.196

65 14:02:26.039 11/05/2001 Sev=Decode/11 IKE/0x43000001

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Aggressive Mode

Flags: (Encryption)

MessageID: 00000000

Length: 469762048

Payload Hash

Next Payload: Notification

Reserved: 0000

Payload Length: 20

Data: 09E5321B10682CCF4C87EDE7EC41E3810000001C

Payload Notification

Next Payload: None

Reserved: 0000

Payload Length: 28

DOI: IPsec

Protocol-ID: PROTO\_ISAKMP

Spi Size: 16

Notify Type: STATUS\_INITIAL\_CONTACT

SPI: DACB1B32139742E7630E88F067C1B0B5

Data:

66 14:02:26.081 11/05/2001 Sev=Info/5 IKE/0x4300002F

Received ISAKMP packet: peer = 161.44.127.196

67 14:02:26.081 11/05/2001 Sev=Debug/7 IKE/0x43000022

Crypto READY becoming ACTIVE

68 14:02:26.084 11/05/2001 Sev=Decode/11 IKE/0x43000001

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Transaction

Flags: (Encryption)

MessageID: D16C4008

Length: 100

Payload Hash

Next Payload: Attributes

Reserved: 0000

Payload Length: 20

Data: EFB8FABB63311D72DDB7F15A809215B700000034

Payload Attributes

Next Payload: None

Reserved: 0000

Payload Length: 52

type: ISAKMP\_CFG\_REQUEST

Reserved: 00

Identifier: 0000

XAUTH Type: RADIUS-CHAP

XAUTH User Name: (empty)

XAUTH User Password: (empty)

XAUTH Message: (data not displayed)

69 14:02:26.084 11/05/2001 Sev=Info/4 IKE/0x43000014

RECEIVING <<< ISAKMP OAK TRANS \*(HASH, ATTR) from  
161.44.127.196

70 14:02:26.084 11/05/2001 Sev=Info/4 CM/0x43100015

Launch xAuth application

71 14:02:27.098 11/05/2001 Sev=Info/4 IPSEC/0x43700012

Delete all keys associated with peer 161.44.127.194

72 14:02:27.098 11/05/2001 Sev=Info/4 IPSEC/0x43700014

Deleted all keys

73 14:02:27.098 11/05/2001 Sev=Info/4 IPSEC/0x4370000D

Key(s) deleted by Interface (192.168.10.41)

74 14:02:42.971 11/05/2001 Sev=Info/4 CM/0x43100017

xAuth application returned

75 14:02:42.971 11/05/2001 Sev=Info/4 IKE/0x43000013

SENDING >>> ISAKMP OAK TRANS \*(HASH, ATTR) to 161.44.127.196

76 14:02:42.974 11/05/2001 Sev=Decode/11 IKE/0x43000001

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Transaction



Flags: (Encryption)

MessageID: 08406CD1

Length: 469762048

Payload Hash

Next Payload: Attributes

Reserved: 0000

Payload Length: 20

Data: 0E26F47ABBA0AF052EA3B9DC6E34C9B300000024

Payload Attributes

Next Payload: None

Reserved: 0000

Payload Length: 36

type: ISAKMP\_CFG\_REPLY

Reserved: 00

Identifier: 0000

XAUTH Type: RADIUS-CHAP

XAUTH User Name: (data not displayed)

XAUTH User Password: (data not displayed)

77 14:02:43.819 11/05/2001 Sev=Info/5 IKE/0x4300002F

Received ISAKMP packet: peer = 161.44.127.196

78 14:02:43.822 11/05/2001 Sev=Decode/11 IKE/0x43000001

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Transaction

Flags: (Encryption)

MessageID: 4D49FD67

Length: 60

Payload Hash

Next Payload: Attributes

Reserved: 0000

Payload Length: 20

Data: 20516C85949FEB6061853707A36B730D0000000C

Payload Attributes

Next Payload: None

Reserved: 0000

Payload Length: 12

type: ISAKMP\_CFG\_SET

Reserved: 00

Identifier: 0000

XAUTH Status: Pass

79 14:02:43.822 11/05/2001 Sev=Info/4 IKE/0x43000014

RECEIVING <<< ISAKMP OAK TRANS \*(HASH, ATTR) from  
161.44.127.196

80 14:02:43.822 11/05/2001 Sev=Info/4 CM/0x4310000E

Established Phase 1 SA. 1 Phase 1 SA in the system

81 14:02:43.825 11/05/2001 Sev=Info/4 IKE/0x43000013

SENDING >>> ISAKMP OAK TRANS \*(HASH, ATTR) to 161.44.127.196

82 14:02:43.828 11/05/2001 Sev=Decode/11 IKE/0x43000001

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Transaction

Flags: (Encryption)

MessageID: 67FD494D

Length: 469762048

Payload Hash

Next Payload: Attributes

Reserved: 0000

Payload Length: 20

Data: 80AEFC5EA1F421789068A21B520A1E7700000008

Payload Attributes

Next Payload: None

Reserved: 0000

Payload Length: 8

type: ISAKMP\_CFG\_ACK

Reserved: 00

Identifier: 0000

83 14:02:43.829 11/05/2001 Sev=Info/4 IKE/0x43000013

SENDING >>> ISAKMP OAK TRANS \*(HASH, ATTR) to 161.44.127.196

84 14:02:43.831 11/05/2001 Sev=Decode/11 IKE/0x43000001

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Transaction

Flags: (Encryption)

MessageID: 19973167

Length: 469762048

Payload Hash

Next Payload: Attributes

Reserved: 0000

Payload Length: 20

Data: 9309A365C01503CB0B89B888D530494500000056

Payload Attributes

Next Payload: None

Reserved: 0000

Payload Length: 86

type: ISAKMP\_CFG\_REQUEST

Reserved: 00

Identifier: 0000

IPv4 Address: (empty)

IPv4 Netmask: (empty)

IPv4 DNS: (empty)

IPv4 NBNS (WINS): (empty)

Address Expiry: (empty)

Application Version: Cisco Systems VPN Client 3.0.8

Cisco extension: Banner: (empty)

Cisco extension: Save PWD: (empty)

Cisco extension: Default Domain Name: (empty)

Cisco extension: Split Include: (empty)

Cisco extension: Do PFS: (empty)

Cisco extension: NAT traversal UDP Port: (empty)

85 14:02:43.832 11/05/2001 Sev=Debug/8 IKE/0x4300004B

Starting DPD timer for IKE SA\* 081801C8, sa->state = 4,  
sa->dpd\_peer\_enabled = 1, sa->dpd\_timer = 081803FC,  
sa->dpd.worry\_freq = 5000

86 14:02:43.879 11/05/2001 Sev=Info/5 IKE/0x4300002F

Received ISAKMP packet: peer = 161.44.127.196

87 14:02:43.882 11/05/2001 Sev=Decode/11 IKE/0x43000001

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Transaction

Flags: (Encryption)

MessageID: 67319719

Length: 236

Payload Hash

Next Payload: Attributes

Reserved: 0000

Payload Length: 20

Data: 8722B4CDB825174DAB03CBC052241CC600000B7

Payload Attributes

Next Payload: None

Reserved: 0000

Payload Length: 183

type: ISAKMP\_CFG\_REPLY

Reserved: 00

Identifier: 0000

IPv4 Address: 4.0.0.0

IPv4 DNS: 4.0.0.0

IPv4 DNS: 4.0.0.0

IPv4 NBNS (WINS): 4.0.0.0

IPv4 NBNS (WINS): 4.0.0.0

Cisco extension: Banner: rtp-vpn-cluster-2-nat:  
Cisco Systems Inc.

UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.

Cisco extension: Save PWD: No

Cisco extension: Default Domain Name: cisco.com

Cisco extension: NAT traversal UDP Port: 3221200488

Cisco extension: Do PFS: No

88 14:02:43.882 11/05/2001 Sev=Info/4 IKE/0x43000014

RECEIVING <<< ISAKMP OAK TRANS \*(HASH, ATTR) from  
161.44.127.196

89 14:02:43.883 11/05/2001 Sev=Info/5 IKE/0x43000010

MODE\_CFG\_REPLY: Attribute = INTERNAL\_IPV4\_ADDRESS: ,  
value = 10.82.240.214

90 14:02:43.883 11/05/2001 Sev=Info/5 IKE/0x43000010

MODE\_CFG\_REPLY: Attribute = INTERNAL\_IPV4\_DNS(1): ,  
value = 64.102.6.247

91 14:02:43.883 11/05/2001 Sev=Info/5 IKE/0x43000010

MODE\_CFG\_REPLY: Attribute = INTERNAL\_IPV4\_DNS(2): ,

value = 171.68.226.120

92 14:02:43.883 11/05/2001 Sev=Info/5 IKE/0x43000010

MODE\_CFG\_REPLY: Attribute = INTERNAL\_IPV4\_NBNS(1)  
(a.k.a. WINS) : , value = 64.102.2.124

93 14:02:43.883 11/05/2001 Sev=Info/5 IKE/0x43000010

MODE\_CFG\_REPLY: Attribute = INTERNAL\_IPV4\_NBNS(2)  
(a.k.a. WINS): , value = 171.68.235.228

94 14:02:43.883 11/05/2001 Sev=Info/5 IKE/0x4300000E

MODE\_CFG\_REPLY: Attribute = MODECFG\_UNITY\_BANNER,  
value = rtp-vpn-cluster-2-nat: Cisco Systems Inc.

UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.

95 14:02:43.883 11/05/2001 Sev=Info/5 IKE/0x4300000D

MODE\_CFG\_REPLY: Attribute = MODECFG\_UNITY\_SAVEPWD: ,  
value = 0x00000000

96 14:02:43.883 11/05/2001 Sev=Info/5 IKE/0x4300000E

MODE\_CFG\_REPLY: Attribute = MODECFG\_UNITY\_DEFDOMAIN: ,  
value = cisco.com

97 14:02:43.883 11/05/2001 Sev=Info/5 IKE/0x4300000D

MODE\_CFG\_REPLY: Attribute = MODECFG\_UNITY\_UDP\_NAT\_PORT,  
value = 0x00002710

98 14:02:43.883 11/05/2001 Sev=Info/5 IKE/0x4300000D

MODE\_CFG\_REPLY: Attribute = MODECFG\_UNITY\_PFS: ,  
value = 0x00000000

99 14:02:43.899 11/05/2001 Sev=Info/4 CM/0x43100019

Mode Config data received

100 14:03:03.938 11/05/2001 Sev=Info/5 IKE/0x43000055

Received a key request from Driver for IP address  
161.44.127.196, GW IP = 161.44.127.196

101 14:03:03.939 11/05/2001 Sev=Info/4 IKE/0x43000013

SENDING >>> ISAKMP OAK QM \*(HASH, SA, NON, ID, ID)  
to 161.44.127.196

102 14:03:03.942 11/05/2001 Sev=Decode/11 IKE/0x43000001

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Quick Mode

Flags: (Encryption)

MessageID: 371035BB

Length: 469762048

Payload Hash

Next Payload: Security Association

Reserved: 0000

Payload Length: 20

Data: C4134662EC838D6032DC22393A14ECA90A0002B8

Payload Security Association

Next Payload: Nonce

Reserved: 0000

Payload Length: 696

DOI: IPsec

Situation: (SIT\_IDENTITY\_ONLY)

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 1

Protocol-Id: PROTO\_IPSEC\_ESP

SPI Size: 4

# of transforms: 1

SPI: 76AF9EAA

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP\_3DES

Reserved2: 0000

Authentication Algorithm: MD5

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 34

Proposal #: 1

Protocol-Id: PROTO\_IPCOMP

SPI Size: 2

# of transforms: 1

SPI: 11B2

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 24

Transform #: 1

Transform-Id: IPCOMP\_LZS

Reserved2: 0000

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 2

Protocol-Id: PROTO\_IPSEC\_ESP

SPI Size: 4

# of transforms: 1

SPI: 76AF9EAA



Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP\_3DES

Reserved2: 0000

Authentication Algorithm: SHA1

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 34

Proposal #: 2

Protocol-Id: PROTO\_IPCOMP

SPI Size: 2

# of transforms: 1

SPI: 2AC8

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 24

Transform #: 1

Transform-Id: IPCOMP\_LZS

Reserved2: 0000

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 3

Protocol-Id: PROTO\_IPSEC\_ESP

SPI Size: 4

# of transforms: 1

SPI: 76AF9EAA

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP\_3DES

Reserved2: 0000

Authentication Algorithm: MD5

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 4

Protocol-Id: PROTO\_IPSEC\_ESP

SPI Size: 4

# of transforms: 1

SPI: 76AF9EAA

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP\_3DES

Reserved2: 0000

Authentication Algorithm: SHA1

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 5

Protocol-Id: PROTO\_IPSEC\_ESP

SPI Size: 4

# of transforms: 1

SPI: 76AF9EAA

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP\_DES

Reserved2: 0000

Authentication Algorithm: MD5

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 34

Proposal #: 5

Protocol-Id: PROTO\_IPCOMP

SPI Size: 2

# of transforms: 1

SPI: 2A25

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 24

Transform #: 1

Transform-Id: IPCOMP\_LZS

Reserved2: 0000

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 6

Protocol-Id: PROTO\_IPSEC\_ESP

SPI Size: 4

# of transforms: 1

SPI: 76AF9EAA

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP\_DES

Reserved2: 0000

Authentication Algorithm: SHA1

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 34

Proposal #: 6

Protocol-Id: PROTO\_IPCOMP

SPI Size: 2

# of transforms: 1

SPI: B7EB

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 24

Transform #: 1

Transform-Id: IPCOMP\_LZS

Reserved2: 0000

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 7

Protocol-Id: PROTO\_IPSEC\_ESP

SPI Size: 4

# of transforms: 1

SPI: 76AF9EAA

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP\_DES

Reserved2: 0000

Authentication Algorithm: MD5

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 8

Protocol-Id: PROTO\_IPSEC\_ESP

SPI Size: 4

# of transforms: 1

SPI: 76AF9EAA

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP\_DES

Reserved2: 0000

Authentication Algorithm: SHA1

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 9

Protocol-Id: PROTO\_IPSEC\_ESP

SPI Size: 4

# of transforms: 1

SPI: 76AF9EAA

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP\_NULL

Reserved2: 0000

Authentication Algorithm: MD5

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 34

Proposal #: 9

Protocol-Id: PROTO\_IPCOMP

SPI Size: 2

# of transforms: 1

SPI: 9637

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 24

Transform #: 1

Transform-Id: IPCOMP\_LZS

Reserved2: 0000

Encapsulation Mode: Tunnel  
Life Type: Seconds  
Life Duration (Hex): 0020C49B  
Payload Proposal  
Next Payload: Proposal  
Reserved: 0000  
Payload Length: 40  
Proposal #: 10  
Protocol-Id: PROTO\_IPSEC\_ESP  
SPI Size: 4  
# of transforms: 1  
SPI: 76AF9EAA  
Payload Transform  
Next Payload: None  
Reserved: 0000  
Payload Length: 28  
Transform #: 1  
Transform-Id: ESP\_NULL  
Reserved2: 0000  
Authentication Algorithm: SHA1  
Encapsulation Mode: Tunnel  
Life Type: Seconds  
Life Duration (Hex): 0020C49B  
Payload Proposal  
Next Payload: Proposal  
Reserved: 0000  
Payload Length: 34  
Proposal #: 10  
Protocol-Id: PROTO\_IPCOMP  
SPI Size: 2  
# of transforms: 1  
SPI: 68E9



Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 24

Transform #: 1

Transform-Id: IPCOMP\_LZS

Reserved2: 0000

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 11

Protocol-Id: PROTO\_IPSEC\_ESP

SPI Size: 4

# of transforms: 1

SPI: 76AF9EAA

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP\_NULL

Reserved2: 0000

Authentication Algorithm: MD5

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: None

Reserved: 0000

Payload Length: 40

Proposal #: 12

Protocol-Id: PROTO\_IPSEC\_ESP

SPI Size: 4

# of transforms: 1

SPI: 76AF9EAA

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP\_NULL

Reserved2: 0000

Authentication Algorithm: SHA1

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Nonce

Next Payload: Identification

Reserved: 0000

Payload Length: 24

Data: B63EA44802CE0827FDEEEEC71751188416F73CE30500000C

Payload Identification

Next Payload: Identification

Reserved: 0000

Payload Length: 12

ID Type: IPv4 Address

Protocol ID (UDP/TCP, etc...): 0

Port: 0

ID Data: 10.82.240.214

Payload Identification

Next Payload: None

Reserved: 0000

Payload Length: 12

ID Type: IPv4 Address

Protocol ID (UDP/TCP, etc...): 0

Port: 0

ID Data: 161.44.127.196

103 14:03:03.943 11/05/2001 Sev=Info/5 IKE/0x43000055

Received a key request from Driver for IP address  
10.10.10.255, GW IP = 161.44.127.196

104 14:03:03.944 11/05/2001 Sev=Info/4 IKE/0x43000013

SENDING >>> ISAKMP OAK QM \*(HASH, SA, NON, ID, ID)  
to 161.44.127.196

105 14:03:03.947 11/05/2001 Sev=Decode/11 IKE/0x43000001

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Quick Mode

Flags: (Encryption)

MessageID: F94C749C

Length: 469762048

Payload Hash

Next Payload: Security Association

Reserved: 0000

Payload Length: 20

Data: 7FEE58A44DA5DC279D9DE7D1C8651ED80A0002B8

Payload Security Association

Next Payload: Nonce

Reserved: 0000

Payload Length: 696

DOI: IPsec

Situation: (SIT\_IDENTITY\_ONLY)

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 1

Protocol-Id: PROTO\_IPSEC\_ESP

SPI Size: 4

# of transforms: 1

SPI: 47269429

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP\_3DES

Reserved2: 0000

Authentication Algorithm: MD5

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 34

Proposal #: 1

Protocol-Id: PROTO\_IPCOMP

SPI Size: 2

# of transforms: 1

SPI: 37A9

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 24

Transform #: 1

Transform-Id: IPCOMP\_LZS

Reserved2: 0000

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 2

Protocol-Id: PROTO\_IPSEC\_ESP

SPI Size: 4

# of transforms: 1

SPI: 47269429

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP\_3DES

Reserved2: 0000

Authentication Algorithm: SHA1

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 34

Proposal #: 2

Protocol-Id: PROTO\_IPCOMP

SPI Size: 2

# of transforms: 1

SPI: D8C8

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 24

Transform #: 1

Transform-Id: IPCOMP\_LZS

Reserved2: 0000

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 3

Protocol-Id: PROTO\_IPSEC\_ESP

SPI Size: 4

# of transforms: 1

SPI: 47269429

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP\_3DES

Reserved2: 0000

Authentication Algorithm: MD5

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 4

Protocol-Id: PROTO\_IPSEC\_ESP

SPI Size: 4

# of transforms: 1

SPI: 47269429

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP\_3DES

Reserved2: 0000

Authentication Algorithm: SHA1

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 5

Protocol-Id: PROTO\_IPSEC\_ESP

SPI Size: 4

# of transforms: 1

SPI: 47269429

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP\_DES

Reserved2: 0000

Authentication Algorithm: MD5

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 34

Proposal #: 5

Protocol-Id: PROTO\_IPCOMP

SPI Size: 2

# of transforms: 1

SPI: B4AA

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 24

Transform #: 1

Transform-Id: IPCOMP\_LZS

Reserved2: 0000

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal



Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 6

Protocol-Id: PROTO\_IPSEC\_ESP

SPI Size: 4

# of transforms: 1

SPI: 47269429

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP\_DES

Reserved2: 0000

Authentication Algorithm: SHA1

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 34

Proposal #: 6

Protocol-Id: PROTO\_IPCOMP

SPI Size: 2

# of transforms: 1

SPI: 10D5

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 24

Transform #: 1

Transform-Id: IPCOMP\_LZS

Reserved2: 0000

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 7

Protocol-Id: PROTO\_IPSEC\_ESP

SPI Size: 4

# of transforms: 1

SPI: 47269429

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP\_DES

Reserved2: 0000

Authentication Algorithm: MD5

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 8

Protocol-Id: PROTO\_IPSEC\_ESP

SPI Size: 4  
# of transforms: 1  
SPI: 47269429  
Payload Transform  
Next Payload: None  
Reserved: 0000  
Payload Length: 28  
Transform #: 1  
Transform-Id: ESP\_DES  
Reserved2: 0000  
Authentication Algorithm: SHA1  
Encapsulation Mode: Tunnel  
Life Type: Seconds  
Life Duration (Hex): 0020C49B  
Payload Proposal  
Next Payload: Proposal  
Reserved: 0000  
Payload Length: 40  
Proposal #: 9  
Protocol-Id: PROTO\_IPSEC\_ESP  
SPI Size: 4  
# of transforms: 1  
SPI: 47269429  
Payload Transform  
Next Payload: None  
Reserved: 0000  
Payload Length: 28  
Transform #: 1  
Transform-Id: ESP\_NULL  
Reserved2: 0000  
Authentication Algorithm: MD5  
Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 34

Proposal #: 9

Protocol-Id: PROTO\_IPCOMP

SPI Size: 2

# of transforms: 1

SPI: 6A1B

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 24

Transform #: 1

Transform-Id: IPCOMP\_LZS

Reserved2: 0000

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 10

Protocol-Id: PROTO\_IPSEC\_ESP

SPI Size: 4

# of transforms: 1

SPI: 47269429

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP\_NULL

Reserved2: 0000

Authentication Algorithm: SHA1

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 34

Proposal #: 10

Protocol-Id: PROTO\_IPCOMP

SPI Size: 2

# of transforms: 1

SPI: 784E

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 24

Transform #: 1

Transform-Id: IPCOMP\_LZS

Reserved2: 0000

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: Proposal

Reserved: 0000

Payload Length: 40

Proposal #: 11

Protocol-Id: PROTO\_IPSEC\_ESP

SPI Size: 4

# of transforms: 1

SPI: 47269429

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP\_NULL

Reserved2: 0000

Authentication Algorithm: MD5

Encapsulation Mode: Tunnel

Life Type: Seconds

Life Duration (Hex): 0020C49B

Payload Proposal

Next Payload: None

Reserved: 0000

Payload Length: 40

Proposal #: 12

Protocol-Id: PROTO\_IPSEC\_ESP

SPI Size: 4

# of transforms: 1

SPI: 47269429

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP\_NULL

Reserved2: 0000

Authentication Algorithm: SHA1  
Encapsulation Mode: Tunnel  
Life Type: Seconds  
Life Duration (Hex): 0020C49B  
Payload Nonce  
Next Payload: Identification  
Reserved: 0000  
Payload Length: 24  
Data: DCDE51C03B32B7694D2125080EFD647FADD61DDC0500000C  
Payload Identification  
Next Payload: Identification  
Reserved: 0000  
Payload Length: 12  
ID Type: IPv4 Address  
Protocol ID (UDP/TCP, etc...): 0  
Port: 0  
ID Data: 10.82.240.214  
Payload Identification  
Next Payload: None  
Reserved: 0000  
Payload Length: 16  
ID Type: IPv4 Subnet  
Protocol ID (UDP/TCP, etc...): 0  
Port: 0  
ID Data: 0.0.0.0/0.0.0.0

106 14:03:03.948 11/05/2001 Sev=Debug/8 IKE/0x4300004B

Starting DPD timer for IKE SA\* 081801C8, sa->state = 4,  
sa->dpd\_peer\_enabled = 1, sa->dpd\_timer = 081803FC,  
sa->dpd.worry\_freq = 5000

107 14:03:03.948 11/05/2001 Sev=Info/5 IKE/0x4300002F

Received ISAKMP packet: peer = 161.44.127.196

108 14:03:03.951 11/05/2001 Sev=Decode/11 IKE/0x43000001

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Transaction

Flags: (Encryption)

MessageID: 67319719

Length: 236

PACKET MAY BE CORRUPT... RESERVED FIELD NOT SET TO ZERO

109 14:03:03.952 11/05/2001 Sev=Info/4 IKE/0x43000014

RECEIVING <<< ISAKMP OAK TRANS \*(HASH, ) from 161.44.127.196

110 14:03:03.952 11/05/2001 Sev=Warning/3 IKE/0x83000057

Received malformed message or negotiation no longer active  
(message id: 0x67319719)

111 14:03:03.952 11/05/2001 Sev=Info/5 IKE/0x4300002F

Received ISAKMP packet: peer = 161.44.127.196

112 14:03:03.955 11/05/2001 Sev=Decode/11 IKE/0x43000001

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Transaction

Flags: (Encryption)

MessageID: 67319719

Length: 236

PACKET MAY BE CORRUPT... RESERVED FIELD NOT SET TO ZERO

113 14:03:03.955 11/05/2001 Sev=Info/4 IKE/0x43000014

RECEIVING <<< ISAKMP OAK TRANS \*(HASH, ) from 161.44.127.196

114 14:03:03.955 11/05/2001 Sev=Warning/3 IKE/0x83000057

Received malformed message or negotiation no longer active  
(message id: 0x67319719)



115 14:03:03.955 11/05/2001 Sev=Info/4 IPSEC/0x43700014

Deleted all keys

116 14:03:03.955 11/05/2001 Sev=Info/4 IPSEC/0x43700010

Created a new key structure

117 14:03:03.955 11/05/2001 Sev=Info/5 IKE/0x43000055

Received a key request from Driver for IP address 24.93.67.64,  
GW IP = 161.44.127.196

118 14:03:03.955 11/05/2001 Sev=Warning/3 IKE/0xC3000002

Function initialize\_qm failed with an error code of 0x00000000  
(INITIATE:805)

119 14:03:03.990 11/05/2001 Sev=Info/5 IKE/0x4300002F

Received ISAKMP packet: peer = 161.44.127.196

120 14:03:03.993 11/05/2001 Sev=Decode/11 IKE/0x43000001

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Informational

Flags: (Encryption)

MessageID: D10A6912

Length: 92

Payload Hash

Next Payload: Notification

Reserved: 0000

Payload Length: 20

Data: 52138C38D364E77DB5980565F7A8C8EF00000028

Payload Notification

Next Payload: None

Reserved: 0000

Payload Length: 40

DOI: IPsec

Protocol-ID: PROTO\_ISAKMP

Spi Size: 16

Notify Type: STATUS\_RESP\_LIFETIME

SPI: DACB1B32139742E7630E88F067C1B0B5

Data: 800B0001000C000400015180

121 14:03:03.994 11/05/2001 Sev=Info/4 IKE/0x43000014

RECEIVING <<< ISAKMP OAK INFO \*(HASH, NOTIFY:STATUS\_RESP\_LIFETIME)  
from 161.44.127.196

122 14:03:03.994 11/05/2001 Sev=Info/5 IKE/0x43000044

RESPONDER-LIFETIME notify has value of 86400 seconds

123 14:03:03.994 11/05/2001 Sev=Info/5 IKE/0x43000046

This SA has already been alive for 38 seconds, setting expiry to  
86362 seconds from now

124 14:03:03.994 11/05/2001 Sev=Info/5 IKE/0x4300002F

Received ISAKMP packet: peer = 161.44.127.196

125 14:03:03.997 11/05/2001 Sev=Decode/11 IKE/0x43000001

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Quick Mode

Flags: (Encryption)

MessageID: BB351037

Length: 172

Payload Hash

Next Payload: Security Association

Reserved: 0000

Payload Length: 20

Data: 3A6CD2078E1F4CF6ACC2810A77A88BF90A000034

Payload Security Association

Next Payload: Nonce

Reserved: 0000

Payload Length: 52

DOI: IPsec

Situation: (SIT\_IDENTITY\_ONLY)

Payload Proposal

Next Payload: None

Reserved: 0000

Payload Length: 40

Proposal #: 1

Protocol-Id: PROTO\_IPSEC\_ESP

SPI Size: 4

# of transforms: 1

SPI: 0C38AE25

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP\_3DES

Reserved2: 0000

Life Type: Seconds

Life Duration (Hex): 0020C49B

Encapsulation Mode: Tunnel

Authentication Algorithm: MD5

Payload Nonce

Next Payload: Identification

Reserved: 0000

Payload Length: 24

Data: 57184AEFF363B10FC00D05A543D6B0B01067274F0500000C

Payload Identification

Next Payload: Identification

Reserved: 0000

Payload Length: 12

ID Type: IPv4 Address

Protocol ID (UDP/TCP, etc...): 0

Port: 0

ID Data: 10.82.240.214

Payload Identification

Next Payload: Notification

Reserved: 0000

Payload Length: 12

ID Type: IPv4 Address

Protocol ID (UDP/TCP, etc...): 0

Port: 0

ID Data: 161.44.127.196

Payload Notification

Next Payload: None

Reserved: 0000

Payload Length: 24

DOI: IPsec

Protocol-ID: PROTO\_IPSEC\_ESP

Spi Size: 4

Notify Type: STATUS\_RESP\_LIFETIME

SPI: 0C38AE25

Data: 8001000180027080

126 14:03:03.997 11/05/2001 Sev=Info/4 IKE/0x43000014

RECEIVING <<< ISAKMP OAK QM \*(HASH, SA, NON, ID, ID,  
NOTIFY:STATUS\_RESP\_LIFETIME) from 161.44.127.196

127 14:03:03.997 11/05/2001 Sev=Info/5 IKE/0x43000044

RESPONDER-LIFETIME notify has value of 28800 seconds

128 14:03:03.997 11/05/2001 Sev=Info/4 IKE/0x43000013

SENDING >>> ISAKMP OAK QM \*(HASH) to 161.44.127.196

129 14:03:03.1000 11/05/2001 Sev=Decode/11 IKE/0x43000001

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Quick Mode

Flags: (Encryption)

MessageID: 371035BB

Length: 469762048

Payload Hash

Next Payload: None

Reserved: 0000

Payload Length: 20

Data: C2456940045DC9C608E0D4D6FA62822400000000

130 14:03:03.1000 11/05/2001 Sev=Info/5 IKE/0x43000058

Loading IPsec SA (Message ID = 0xBB351037 OUTBOUND SPI =  
0x0C38AE25 INBOUND SPI = 0x76AF9EAA)

131 14:03:04.001 11/05/2001 Sev=Info/5 IKE/0x43000025

Loaded OUTBOUND ESP SPI: 0x0C38AE25

132 14:03:04.001 11/05/2001 Sev=Info/5 IKE/0x43000026

Loaded INBOUND ESP SPI: 0x76AF9EAA

133 14:03:04.001 11/05/2001 Sev=Info/4 CM/0x4310001A

One secure connection established

134 14:03:04.007 11/05/2001 Sev=Info/5 IKE/0x4300002F

Received ISAKMP packet: peer = 161.44.127.196

135 14:03:04.010 11/05/2001 Sev=Decode/11 IKE/0x43000001

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Quick Mode

Flags: (Encryption)

MessageID: 9C744CF9

Length: 180

Payload Hash

Next Payload: Security Association

Reserved: 0000

Payload Length: 20

Data: 4591C989262C4F863FD2DC911E7DBA900A000034

Payload Security Association

Next Payload: Nonce

Reserved: 0000

Payload Length: 52

DOI: IPsec

Situation:(SIT\_IDENTITY\_ONLY)

Payload Proposal

Next Payload: None

Reserved: 0000

Payload Length: 40

Proposal #: 1

Protocol-Id: PROTO\_IPSEC\_ESP

SPI Size: 4

# of transforms: 1

SPI: 503F4CC5

Payload Transform

Next Payload: None

Reserved: 0000

Payload Length: 28

Transform #: 1

Transform-Id: ESP\_3DES

Reserved2: 0000

Life Type: Seconds

Life Duration (Hex): 0020C49B

Encapsulation Mode: Tunnel

Authentication Algorithm: MD5

Payload Nonce

Next Payload: Identification

Reserved: 0000

Payload Length: 24

Data: 4DD4873137DD4765208FFCE6087D30A48FA9634F0500000C

Payload Identification

Next Payload: Identification

Reserved: 0000

Payload Length: 12

ID Type: IPv4 Address

Protocol ID (UDP/TCP, etc...): 0

Port: 0

ID Data: 10.82.240.214

Payload Identification

Next Payload: Notification

Reserved: 0000

Payload Length: 16

ID Type: IPv4 Subnet

Protocol ID (UDP/TCP, etc...): 0

Port: 0

ID Data: 0.0.0.0/0.0.0.0

Payload Notification

Next Payload: None

Reserved: 0000

Payload Length: 24

DOI: IPsec

Protocol-ID: PROTO\_IPSEC\_ESP

Spi Size: 4

Notify Type: STATUS\_RESP\_LIFETIME

SPI: 503F4CC5

Data: 8001000180027080

136 14:03:04.011 11/05/2001 Sev=Info/4 IKE/0x43000014  
RECEIVING <<< ISAKMP OAK QM \*(HASH, SA, NON, ID, ID,  
NOTIFY:STATUS\_RESP\_LIFETIME) from 161.44.127.196

137 14:03:04.011 11/05/2001 Sev=Info/5 IKE/0x43000044  
RESPONDER-LIFETIME notify has value of 28800 seconds

138 14:03:04.011 11/05/2001 Sev=Info/4 IKE/0x43000013  
SENDING >>> ISAKMP OAK QM \*(HASH) to 161.44.127.196

139 14:03:04.014 11/05/2001 Sev=Decode/11 IKE/0x43000001  
ISAKMP Header  
Initiator COOKIE: DACB1B32139742E7  
Responder COOKIE: 630E88F067C1B0B5  
Next Payload: Hash  
Ver: 10  
Exchange Type: Quick Mode  
Flags: (Encryption)  
MessageID: F94C749C  
Length: 469762048  
Payload Hash  
Next Payload: None  
Reserved: 0000  
Payload Length: 20  
Data: 8AF3A2608A24AB1FB8C8ECA82B2CC99200000000

140 14:03:04.014 11/05/2001 Sev=Info/5 IKE/0x43000058  
Loading IPsec SA (Message ID = 0x9C744CF9 OUTBOUND SPI =  
0x503F4CC5 INBOUND SPI = 0x47269429)

141 14:03:04.015 11/05/2001 Sev=Info/5 IKE/0x43000025  
Loaded OUTBOUND ESP SPI: 0x503F4CC5

142 14:03:04.015 11/05/2001 Sev=Info/5 IKE/0x43000026  
Loaded INBOUND ESP SPI: 0x47269429

143 14:03:04.015 11/05/2001 Sev=Info/4 CM/0x43100022  
Additional Phase 2 SA established.

144 14:03:05.018 11/05/2001 Sev=Info/4 IPSEC/0x43700010  
Created a new key structure



145 14:03:05.018 11/05/2001 Sev=Info/4 IPSEC/0x4370000F  
Added key with SPI=0x25ae380c into key list

146 14:03:05.018 11/05/2001 Sev=Info/4 IPSEC/0x43700010  
Created a new key structure

147 14:03:05.018 11/05/2001 Sev=Info/4 IPSEC/0x4370000F  
Added key with SPI=0xaa9eaf76 into key list

148 14:03:05.018 11/05/2001 Sev=Info/4 IPSEC/0x4370000F  
Added key with SPI=0xc54c3f50 into key list

149 14:03:05.019 11/05/2001 Sev=Info/4 IPSEC/0x43700010  
Created a new key structure

150 14:03:05.019 11/05/2001 Sev=Info/4 IPSEC/0x4370000F  
Added key with SPI=0x29942647 into key list

151 14:03:55.528 11/05/2001 Sev=Info/6 IKE/0x4300003D  
Sending DPD request to 161.44.127.196, seq# = 1153554501

152 14:03:55.529 11/05/2001 Sev=Info/4 IKE/0x43000013  
SENDING >>> ISAKMP OAK INFO \*(HASH, NOTIFY:DPD\_REQUEST)  
to 161.44.127.196

153 14:03:55.531 11/05/2001 Sev=Decode/11 IKE/0x43000001  
ISAKMP Header  
Initiator COOKIE: DACB1B32139742E7  
Responder COOKIE: 630E88F067C1B0B5  
Next Payload: Hash  
Ver: 10  
Exchange Type: Informational  
Flags: (Encryption)  
MessageID: 791ED04C  
Length: 469762048  
Payload Hash  
Next Payload: Notification  
Reserved: 0000  
Payload Length: 20  
Data: C0E66CDA100E9C77C75A46AD3AECA51C00000020

Payload Notification

Next Payload: None

Reserved: 0000

Payload Length: 32

DOI: IPsec

Protocol-ID: PROTO\_ISAKMP

Spi Size: 16

Notify Type: DPD\_R\_U\_THERE

SPI: DACB1B32139742E7630E88F067C1B0B5

Data: 44C1D845

154 14:03:55.532 11/05/2001 Sev=Info/4 IKE/0x43000013

SENDING >>> ISAKMP OAK INFO \*(HASH, NOTIFY:HEARTBEAT)  
to 161.44.127.196

155 14:03:55.535 11/05/2001 Sev=Decode/11 IKE/0x43000001

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Informational

Flags: (Encryption)

MessageID: 68218ECF

Length: 469762048

Payload Hash

Next Payload: Notification

Reserved: 0000

Payload Length: 20

Data: E705E1CE2854A92CA7DEC4C04AB6654B0000001C

Payload Notification

Next Payload: None

Reserved: 0000

Payload Length: 28

DOI: IPsec

Protocol-ID: PROTO\_ISAKMP

Spi Size: 16

Notify Type: STATUS\_ALTIGA\_KEEPALIVE

SPI: DACB1B32139742E7630E88F067C1B0B5

Data:

156 14:03:55.535 11/05/2001 Sev=Info/6 IKE/0x43000052

Sent a ping on the IKE SA

157 14:03:55.575 11/05/2001 Sev=Info/5 IKE/0x4300002F

Received ISAKMP packet: peer = 161.44.127.196

158 14:03:55.578 11/05/2001 Sev=Decode/11 IKE/0x43000001

ISAKMP Header

Initiator COOKIE: DACB1B32139742E7

Responder COOKIE: 630E88F067C1B0B5

Next Payload: Hash

Ver: 10

Exchange Type: Informational

Flags: (Encryption)

MessageID: E63FE567

Length: 84

Payload Hash

Next Payload: Notification

Reserved: 0000

Payload Length: 20

Data: FD8DA190626611087DD2B8DC3DDDE72900000020

Payload Notification

Next Payload: None

Reserved: 0000

Payload Length: 32

DOI: IPsec

Protocol-ID: PROTO\_ISAKMP

Spi Size: 16

Notify Type: DPD\_R\_U\_THERE\_ACK

SPI: DACB1B32139742E7630E88F067C1B0B5

Data: 44C1D845

159 14:03:55.579 11/05/2001 Sev=Info/4 IKE/0x43000014

RECEIVING <<< ISAKMP OAK INFO \*(HASH, NOTIFY:DPD\_ACK)  
from 161.44.127.196

160 14:03:55.579 11/05/2001 Sev=Info/5 IKE/0x4300003F

Received DPD ACK from 161.44.127.196, seq# received =  
1153554501, seq# expected = 1153554501

### Concentrateur VPN 3000

1 11/05/2001 14:18:18.630 SEV=8 IKEDBG/0 RPT=199 172.18.124.241

RECEIVED Message (msgid=0) with payloads :  
HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + VENDOR (13)  
+ VENDOR (13) + VENDOR  
(13) + NONE (0) ... total length : 562

4 11/05/2001 14:18:18.630 SEV=9 IKEDBG/0 RPT=200 172.18.124.241

processing SA payload

5 11/05/2001 14:18:18.630 SEV=9 IKEDBG/0 RPT=201 172.18.124.241

processing ke payload

6 11/05/2001 14:18:18.630 SEV=9 IKEDBG/0 RPT=202 172.18.124.241

processing ISA\_KE

7 11/05/2001 14:18:18.630 SEV=9 IKEDBG/1 RPT=59 172.18.124.241

processing nonce payload

8 11/05/2001 14:18:18.630 SEV=9 IKEDBG/1 RPT=60 172.18.124.241

Processing ID

9 11/05/2001 14:18:18.630 SEV=9 IKEDBG/47 RPT=38 172.18.124.241

processing VID payload

10 11/05/2001 14:18:18.630 SEV=9 IKEDBG/49 RPT=37 172.18.124.241

Received xauth V6 VID

11 11/05/2001 14:18:18.630 SEV=9 IKEDBG/47 RPT=39 172.18.124.241

processing VID payload

12 11/05/2001 14:18:18.630 SEV=9 IKEDBG/49 RPT=38 172.18.124.241

Received DPD VID

13 11/05/2001 14:18:18.630 SEV=9 IKEDBG/47 RPT=40 172.18.124.241

processing VID payload

14 11/05/2001 14:18:18.630 SEV=9 IKEDBG/49 RPT=39 172.18.124.241

Received Cisco Unity client VID

15 11/05/2001 14:18:18.630 SEV=9 IKEDBG/23 RPT=12 172.18.124.241

Starting group lookup for peer 172.18.124.241

16 11/05/2001 14:18:18.630 SEV=8 AUTHDBG/1 RPT=4  
AUTH\_Open() returns 3

17 11/05/2001 14:18:18.630 SEV=7 AUTH/12 RPT=4  
Authentication session opened: handle = 3

18 11/05/2001 14:18:18.630 SEV=8 AUTHDBG/3 RPT=6  
AUTH\_PutAttrTable(3, 61ea34)

19 11/05/2001 14:18:18.630 SEV=8 AUTHDBG/6 RPT=3  
AUTH\_GroupAuthenticate(3, 51a88f0, 431480)

20 11/05/2001 14:18:18.630 SEV=8 AUTHDBG/59 RPT=6  
AUTH\_BindServer(511a7bc, 0, 0)

21 11/05/2001 14:18:18.630 SEV=9 AUTHDBG/69 RPT=6  
Auth Server e3199c has been bound to ACB 511a7bc,  
sessions = 1

22 11/05/2001 14:18:18.630 SEV=8 AUTHDBG/65 RPT=6  
AUTH\_CreateTimer(511a7bc, 0, 0)

23 11/05/2001 14:18:18.630 SEV=9 AUTHDBG/72 RPT=6  
Reply timer created: handle = 340017

24 11/05/2001 14:18:18.630 SEV=8 AUTHDBG/61 RPT=6  
AUTH\_BuildMsg(511a7bc, 0, 0)

25 11/05/2001 14:18:18.630 SEV=8 AUTHDBG/64 RPT=6  
AUTH\_StartTimer(511a7bc, 0, 0)

26 11/05/2001 14:18:18.630 SEV=9 AUTHDBG/73 RPT=6  
Reply timer started: handle = 340017, timestamp = 97010941,  
timeout = 30000

27 11/05/2001 14:18:18.630 SEV=8 AUTHDBG/62 RPT=6  
AUTH\_SndRequest(511a7bc, 0, 0)

28 11/05/2001 14:18:18.630 SEV=8 AUTHDBG/50 RPT=11  
IntDB\_Decode(37f34d0, 115)

29 11/05/2001 14:18:18.630 SEV=8 AUTHDBG/47 RPT=11  
IntDB\_Xmt(511a7bc)

30 11/05/2001 14:18:18.630 SEV=9 AUTHDBG/71 RPT=6  
xmit\_cnt = 1

31 11/05/2001 14:18:18.630 SEV=8 AUTHDBG/47 RPT=12  
IntDB\_Xmt(511a7bc)

32 11/05/2001 14:18:18.730 SEV=8 AUTHDBG/49 RPT=6  
IntDB\_Match(511a7bc, 2f1a854)

33 11/05/2001 14:18:18.730 SEV=8 AUTHDBG/63 RPT=6  
AUTH\_RcvReply(511a7bc, 0, 0)

34 11/05/2001 14:18:18.730 SEV=8 AUTHDBG/50 RPT=12  
IntDB\_Decode(2f1a854, 104)

35 11/05/2001 14:18:18.730 SEV=8 AUTHDBG/48 RPT=6  
IntDB\_Rcv(511a7bc)

36 11/05/2001 14:18:18.730 SEV=8 AUTHDBG/66 RPT=6  
AUTH\_DeleteTimer(511a7bc, 0, 0)

37 11/05/2001 14:18:18.730 SEV=9 AUTHDBG/74 RPT=6  
Reply timer stopped: handle = 340017, timestamp = 97010951

38 11/05/2001 14:18:18.730 SEV=8 AUTHDBG/58 RPT=6  
AUTH\_Callback(511a7bc, 0, 0)

39 11/05/2001 14:18:18.730 SEV=6 AUTH/39 RPT=5 172.18.124.241  
Authentication successful: handle = 3, server = Internal,  
group = ipsecgroup

40 11/05/2001 14:18:18.730 SEV=7 IKEDBG/0 RPT=203 172.18.124.241  
Group [ipsecgroup]  
Found Phase 1 Group (ipsecgroup)

41 11/05/2001 14:18:18.730 SEV=8 AUTHDBG/4 RPT=4  
AUTH\_GetAttrTable(3, 61ea7c)

42 11/05/2001 14:18:18.730 SEV=7 IKEDBG/14 RPT=4 172.18.124.241  
Group [ipsecgroup]  
Authentication configured for Internal

43 11/05/2001 14:18:18.730 SEV=8 AUTHDBG/2 RPT=4  
AUTH\_Close(3)

44 11/05/2001 14:18:18.730 SEV=9 IKEDBG/0 RPT=204 172.18.124.241  
Group [ipsecgroup]  
processing IKE SA

45 11/05/2001 14:18:18.730 SEV=8 IKEDBG/0 RPT=205 172.18.124.241  
Group [ipsecgroup]  
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE  
Parsing received transform:  
Phase 1 failure against global IKE proposal # 1:  
Mismatched attr types for class Hash Alg:  
Rcv'd: SHA  
Cfg'd: MD5

50 11/05/2001 14:18:18.730 SEV=8 IKEDBG/0 RPT=206 172.18.124.241  
Group [ipsecgroup]  
Phase 1 failure against global IKE proposal # 2:  
Mismatched attr types for class Hash Alg:  
Rcv'd: SHA  
Cfg'd: MD5

53 11/05/2001 14:18:18.730 SEV=8 IKEDBG/0 RPT=207 172.18.124.241  
Group [ipsecgroup]  
Phase 1 failure against global IKE proposal # 3:  
Mismatched attr types for class Hash Alg:

Rcv'd: SHA  
Cfg'd: MD5

56 11/05/2001 14:18:18.730 SEV=8 IKEDBG/0 RPT=208 172.18.124.241  
Group [ipsecgroup]  
Phase 1 failure against global IKE proposal # 4:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 2  
Cfg'd: Oakley Group 1

60 11/05/2001 14:18:18.730 SEV=8 IKEDBG/0 RPT=209 172.18.124.241  
Group [ipsecgroup]  
Phase 1 failure against global IKE proposal # 5:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 2  
Cfg'd: Oakley Group 1

64 11/05/2001 14:18:18.730 SEV=8 IKEDBG/0 RPT=210 172.18.124.241  
Group [ipsecgroup]  
Phase 1 failure against global IKE proposal # 6:  
Mismatched attr types for class DH Group:  
Rcv'd: Oakley Group 2  
Cfg'd: Oakley Group 7

68 11/05/2001 14:18:18.730 SEV=7 IKEDBG/28 RPT=4 172.18.124.241  
Group [ipsecgroup]  
IKE SA Proposal # 1, Transform # 2 acceptable  
Matches global IKE entry # 1

70 11/05/2001 14:18:18.730 SEV=8 AUTHDBG/60 RPT=6  
AUTH\_UnbindServer(511a7bc, 0, 0)

71 11/05/2001 14:18:18.730 SEV=9 AUTHDBG/70 RPT=6  
Auth Server e3199c has been unbound from ACB 511a7bc, sessions = 0

72 11/05/2001 14:18:18.730 SEV=8 AUTHDBG/10 RPT=4  
AUTH\_Int\_FreeAuthCB(511a7bc)

73 11/05/2001 14:18:18.730 SEV=9 AUTHDBG/19 RPT=4  
instance = 4, clone\_instance = 0

74 11/05/2001 14:18:18.730 SEV=7 AUTH/13 RPT=4  
Authentication session closed: handle = 3

75 11/05/2001 14:18:18.760 SEV=9 IKEDBG/0 RPT=211 172.18.124.241  
Group [ipsecgroup]  
constructing ISA\_SA for isakmp

76 11/05/2001 14:18:18.760 SEV=9 IKEDBG/0 RPT=212 172.18.124.241  
Group [ipsecgroup]  
constructing ke payload

77 11/05/2001 14:18:18.760 SEV=9 IKEDBG/1 RPT=61 172.18.124.241  
Group [ipsecgroup]  
constructing nonce payload

78 11/05/2001 14:18:18.760 SEV=9 IKE/0 RPT=5 172.18.124.241  
Group [ipsecgroup]  
Generating keys for Responder...

79 11/05/2001 14:18:18.760 SEV=9 IKEDBG/1 RPT=62 172.18.124.241  
Group [ipsecgroup]  
constructing ID

80 11/05/2001 14:18:18.760 SEV=9 IKEDBG/0 RPT=213  
Group [ipsecgroup]  
construct hash payload

81 11/05/2001 14:18:18.760 SEV=9 IKEDBG/0 RPT=214 172.18.124.241  
Group [ipsecgroup]  
computing hash

82 11/05/2001 14:18:18.760 SEV=9 IKEDBG/46 RPT=12 172.18.124.241  
Group [ipsecgroup]  
constructing Cisco Unity VID payload

83 11/05/2001 14:18:18.760 SEV=9 IKEDBG/46 RPT=13 172.18.124.241  
Group [ipsecgroup]  
constructing xauth V6 VID payload

84 11/05/2001 14:18:18.760 SEV=9 IKEDBG/46 RPT=14 172.18.124.241  
Group [ipsecgroup]  
constructing dpd vid payload

85 11/05/2001 14:18:18.760 SEV=9 IKEDBG/46 RPT=15 172.18.124.241  
Group [ipsecgroup]  
constructing VID payload

86 11/05/2001 14:18:18.760 SEV=9 IKEDBG/48 RPT=5 172.18.124.241  
Group [ipsecgroup]  
Send Altiga GW VID

87 11/05/2001 14:18:18.760 SEV=8 IKEDBG/0 RPT=215 172.18.124.241  
SENDING Message (msgid=0) with payloads :  
HDR + SA (1) ... total length : 344

88 11/05/2001 14:18:18.790 SEV=8 IKEDBG/0 RPT=216 172.18.124.241  
RECEIVED Message (msgid=0) with payloads :  
HDR + HASH (8) + NOTIFY (11) + NONE (0) ... total length : 76

89 11/05/2001 14:18:18.790 SEV=9 IKEDBG/0 RPT=217 172.18.124.241  
Group [ipsecgroup]  
processing hash

90 11/05/2001 14:18:18.790 SEV=9 IKEDBG/0 RPT=218 172.18.124.241  
Group [ipsecgroup]  
computing hash

91 11/05/2001 14:18:18.790 SEV=9 IKEDBG/0 RPT=219 172.18.124.241  
Group [ipsecgroup]  
Processing Notify payload

92 11/05/2001 14:18:18.790 SEV=9 IKEDBG/0 RPT=220 172.18.124.241  
Group [ipsecgroup]  
constructing blank hash

93 11/05/2001 14:18:18.790 SEV=9 IKEDBG/0 RPT=221 172.18.124.241  
Group [ipsecgroup]  
constructing qm hash

94 11/05/2001 14:18:18.790 SEV=8 IKEDBG/0 RPT=222 172.18.124.241  
SENDING Message (msgid=6ea8e2bc) with payloads :  
HDR + HASH (8) ... total length : 100

95 11/05/2001 14:18:23.290 SEV=8 IKEDBG/0 RPT=223 172.18.124.241  
RECEIVED Message (msgid=6ea8e2bc) with payloads :  
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 85



99 11/05/2001 14:18:23.290 SEV=9 IKEDBG/1 RPT=63  
process\_attr(): Enter!

100 11/05/2001 14:18:23.290 SEV=9 IKEDBG/1 RPT=64  
Processing cfg reply attributes.

101 11/05/2001 14:18:23.290 SEV=8 AUTHDBG/1 RPT=5  
AUTH\_Open() returns 4

102 11/05/2001 14:18:23.290 SEV=7 AUTH/12 RPT=5  
Authentication session opened: handle = 4

103 11/05/2001 14:18:23.290 SEV=8 AUTHDBG/3 RPT=7  
AUTH\_PutAttrTable(4, 61ea34)

104 11/05/2001 14:18:23.290 SEV=8 AUTHDBG/5 RPT=2  
AUTH\_Authenticate(4, 2f1b480, 460ec0)

105 11/05/2001 14:18:23.290 SEV=8 AUTHDBG/59 RPT=7  
AUTH\_BindServer(511760c, 0, 0)

106 11/05/2001 14:18:23.290 SEV=9 AUTHDBG/69 RPT=7  
Auth Server e3199c has been bound to ACB 511760c,  
sessions = 1

107 11/05/2001 14:18:23.290 SEV=8 AUTHDBG/65 RPT=7  
AUTH\_CreateTimer(511760c, 0, 0)

108 11/05/2001 14:18:23.290 SEV=9 AUTHDBG/72 RPT=7  
Reply timer created: handle = 360014

109 11/05/2001 14:18:23.290 SEV=8 AUTHDBG/61 RPT=7  
AUTH\_BuildMsg(511760c, 0, 0)

110 11/05/2001 14:18:23.290 SEV=8 AUTHDBG/64 RPT=7  
AUTH\_StartTimer(511760c, 0, 0)

111 11/05/2001 14:18:23.290 SEV=9 AUTHDBG/73 RPT=7  
Reply timer started: handle = 360014, timestamp =  
97011407, timeout = 30000

112 11/05/2001 14:18:23.290 SEV=8 AUTHDBG/62 RPT=7  
AUTH\_SndRequest(511760c, 0, 0)

113 11/05/2001 14:18:23.290 SEV=8 AUTHDBG/50 RPT=13  
IntDB\_Decode(37f34d0, 102)

114 11/05/2001 14:18:23.290 SEV=8 AUTHDBG/47 RPT=13  
IntDB\_Xmt(511760c)

115 11/05/2001 14:18:23.290 SEV=9 AUTHDBG/71 RPT=7  
xmit\_cnt = 1

116 11/05/2001 14:18:23.290 SEV=8 AUTHDBG/47 RPT=14  
IntDB\_Xmt(511760c)

117 11/05/2001 14:18:23.390 SEV=8 AUTHDBG/49 RPT=7  
IntDB\_Match(511760c, 2f1bb8c)

118 11/05/2001 14:18:23.390 SEV=8 AUTHDBG/63 RPT=7  
AUTH\_RcvReply(511760c, 0, 0)

119 11/05/2001 14:18:23.390 SEV=8 AUTHDBG/50 RPT=14  
IntDB\_Decode(2f1bb8c, 116)

120 11/05/2001 14:18:23.390 SEV=8 AUTHDBG/48 RPT=7  
IntDB\_Rcv(511760c)

121 11/05/2001 14:18:23.390 SEV=8 AUTHDBG/66 RPT=7  
AUTH\_DeleteTimer(511760c, 0, 0)

122 11/05/2001 14:18:23.390 SEV=9 AUTHDBG/74 RPT=7  
Reply timer stopped: handle = 360014, timestamp = 97011417

123 11/05/2001 14:18:23.390 SEV=8 AUTHDBG/58 RPT=7  
AUTH\_Callback(511760c, 0, 0)

124 11/05/2001 14:18:23.390 SEV=6 AUTH/4 RPT=2 172.18.124.241  
Authentication successful: handle = 4, server =  
Internal, user = ipsecuser

125 11/05/2001 14:18:23.390 SEV=8 AUTHDBG/3 RPT=8  
AUTH\_PutAttrTable(4, f0d688)

126 11/05/2001 14:18:23.390 SEV=8 AUTHDBG/60 RPT=7  
AUTH\_UnbindServer(511760c, 0, 0)

127 11/05/2001 14:18:23.390 SEV=9 AUTHDBG/70 RPT=7  
Auth Server e3199c has been unbound from ACB 511760c,  
sessions = 0

128 11/05/2001 14:18:23.390 SEV=8 AUTHDBG/59 RPT=8  
AUTH\_BindServer(511760c, 0, 0)

129 11/05/2001 14:18:23.390 SEV=9 AUTHDBG/69 RPT=8  
Auth Server e3199c has been bound to ACB 511760c,  
sessions = 1

130 11/05/2001 14:18:23.390 SEV=8 AUTHDBG/65 RPT=8  
AUTH\_CreateTimer(511760c, 0, 0)

131 11/05/2001 14:18:23.390 SEV=9 AUTHDBG/72 RPT=8  
Reply timer created: handle = 370014

132 11/05/2001 14:18:23.390 SEV=8 AUTHDBG/61 RPT=8  
AUTH\_BuildMsg(511760c, 0, 0)

133 11/05/2001 14:18:23.390 SEV=8 AUTHDBG/64 RPT=8  
AUTH\_StartTimer(511760c, 0, 0)

134 11/05/2001 14:18:23.390 SEV=9 AUTHDBG/73 RPT=8  
Reply timer started: handle = 370014, timestamp =  
97011417, timeout = 30000

135 11/05/2001 14:18:23.390 SEV=8 AUTHDBG/62 RPT=8  
AUTH\_SndRequest(511760c, 0, 0)

136 11/05/2001 14:18:23.390 SEV=8 AUTHDBG/50 RPT=15  
IntDB\_Decode(1f9d5b8, 44)

137 11/05/2001 14:18:23.390 SEV=8 AUTHDBG/47 RPT=15  
IntDB\_Xmt(511760c)

138 11/05/2001 14:18:23.390 SEV=9 AUTHDBG/71 RPT=8  
xmit\_cnt = 1

139 11/05/2001 14:18:23.390 SEV=8 AUTHDBG/47 RPT=16  
IntDB\_Xmt(511760c)

140 11/05/2001 14:18:23.490 SEV=8 AUTHDBG/49 RPT=8  
IntDB\_Match(511760c, 2f1af60)

141 11/05/2001 14:18:23.490 SEV=8 AUTHDBG/63 RPT=8  
AUTH\_RcvReply(511760c, 0, 0)

142 11/05/2001 14:18:23.490 SEV=8 AUTHDBG/50 RPT=16  
IntDB\_Decode(2f1af60, 104)

143 11/05/2001 14:18:23.490 SEV=8 AUTHDBG/48 RPT=8  
IntDB\_Rcv(511760c)

144 11/05/2001 14:18:23.490 SEV=8 AUTHDBG/66 RPT=8  
AUTH\_DeleteTimer(511760c, 0, 0)

145 11/05/2001 14:18:23.490 SEV=9 AUTHDBG/74 RPT=8  
Reply timer stopped: handle = 370014, timestamp =  
97011427

146 11/05/2001 14:18:23.490 SEV=8 AUTHDBG/58 RPT=8  
AUTH\_Callback(511760c, 0, 0)

147 11/05/2001 14:18:23.490 SEV=6 AUTH/39 RPT=6  
172.18.124.241  
Authentication successful: handle = 4, server =  
Internal, group = ipsecgroup

148 11/05/2001 14:18:23.490 SEV=8 AUTHDBG/3 RPT=9  
AUTH\_PutAttrTable(4, f0d688)

149 11/05/2001 14:18:23.490 SEV=8 AUTHDBG/60 RPT=8  
AUTH\_UnbindServer(511760c, 0, 0)

150 11/05/2001 14:18:23.490 SEV=9 AUTHDBG/70 RPT=8  
Auth Server e3199c has been unbound from ACB 511760c,  
sessions = 0

151 11/05/2001 14:18:23.490 SEV=8 AUTHDBG/59 RPT=9  
AUTH\_BindServer(511760c, 0, 0)

152 11/05/2001 14:18:23.490 SEV=9 AUTHDBG/69 RPT=9  
Auth Server e3199c has been bound to ACB 511760c,  
sessions = 1

153 11/05/2001 14:18:23.490 SEV=8 AUTHDBG/65 RPT=9  
AUTH\_CreateTimer(511760c, 0, 0)

154 11/05/2001 14:18:23.490 SEV=9 AUTHDBG/72 RPT=9  
Reply timer created: handle = 380014

155 11/05/2001 14:18:23.490 SEV=8 AUTHDBG/61 RPT=9  
AUTH\_BuildMsg(511760c, 0, 0)

156 11/05/2001 14:18:23.490 SEV=8 AUTHDBG/64 RPT=9  
AUTH\_StartTimer(511760c, 0, 0)

157 11/05/2001 14:18:23.490 SEV=9 AUTHDBG/73 RPT=9  
Reply timer started: handle = 380014, timestamp =  
97011427, timeout = 30000

158 11/05/2001 14:18:23.490 SEV=8 AUTHDBG/62 RPT=9  
AUTH\_SndRequest(511760c, 0, 0)

159 11/05/2001 14:18:23.490 SEV=8 AUTHDBG/50 RPT=17  
IntDB\_Decode(1fe8cc0, 44)

160 11/05/2001 14:18:23.490 SEV=8 AUTHDBG/47 RPT=17  
IntDB\_Xmt(511760c)

161 11/05/2001 14:18:23.490 SEV=9 AUTHDBG/71 RPT=9  
xmit\_cnt = 1

162 11/05/2001 14:18:23.490 SEV=8 AUTHDBG/47 RPT=18  
IntDB\_Xmt(511760c)

163 11/05/2001 14:18:23.590 SEV=8 AUTHDBG/49 RPT=9  
IntDB\_Match(511760c, 2f1a99c)

164 11/05/2001 14:18:23.590 SEV=8 AUTHDBG/63 RPT=9  
AUTH\_RcvReply(511760c, 0, 0)

165 11/05/2001 14:18:23.590 SEV=8 AUTHDBG/50 RPT=18  
IntDB\_Decode(2f1a99c, 104)

166 11/05/2001 14:18:23.590 SEV=8 AUTHDBG/48 RPT=9  
IntDB\_Rcv(511760c)

167 11/05/2001 14:18:23.590 SEV=8 AUTHDBG/66 RPT=9  
AUTH\_DeleteTimer(511760c, 0, 0)

168 11/05/2001 14:18:23.590 SEV=9 AUTHDBG/74 RPT=9  
Reply timer stopped: handle = 380014, timestamp =  
97011437

169 11/05/2001 14:18:23.590 SEV=8 AUTHDBG/58 RPT=9  
AUTH\_Callback(511760c, 0, 0)

170 11/05/2001 14:18:23.590 SEV=6 AUTH/39 RPT=7  
172.18.124.241  
Authentication successful: handle = 4, server =  
Internal, group = ipsecgroup

171 11/05/2001 14:18:23.590 SEV=8 AUTHDBG/4 RPT=5  
AUTH\_GetAttrTable(4, 61ea7c)

172 11/05/2001 14:18:23.590 SEV=7 IKEDBG/14 RPT=5  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Authentication configured for Internal

173 11/05/2001 14:18:23.590 SEV=8 AUTHDBG/2 RPT=5  
AUTH\_Close(4)

174 11/05/2001 14:18:23.590 SEV=4 IKE/52 RPT=2  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
User (ipsecuser) authenticated.

175 11/05/2001 14:18:23.590 SEV=9 IKEDBG/0 RPT=224  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing blank hash

176 11/05/2001 14:18:23.590 SEV=9 IKEDBG/0 RPT=225  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing qm hash

177 11/05/2001 14:18:23.590 SEV=8 IKEDBG/0 RPT=226  
172.18.124.241  
SENDING Message (msgid=938074b7) with payloads :  
HDR + HASH (8) ... total length : 60

179 11/05/2001 14:18:23.590 SEV=8 AUTHDBG/60 RPT=9  
AUTH\_UnbindServer(511760c, 0, 0)

180 11/05/2001 14:18:23.590 SEV=9 AUTHDBG/70 RPT=9  
Auth Server e3199c has been unbound from ACB 511760c,  
sessions = 0

181 11/05/2001 14:18:23.590 SEV=8 AUTHDBG/10 RPT=5  
AUTH\_Int\_FreeAuthCB(511760c)

182 11/05/2001 14:18:23.590 SEV=9 AUTHDBG/19 RPT=5  
instance = 5, clone\_instance = 0

183 11/05/2001 14:18:23.590 SEV=7 AUTH/13 RPT=5  
Authentication session closed: handle = 4

184 11/05/2001 14:18:23.600 SEV=8 IKEDBG/0 RPT=227  
172.18.124.241  
RECEIVED Message (msgid=938074b7) with payloads :  
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 56

186 11/05/2001 14:18:23.600 SEV=9 IKEDBG/1 RPT=65  
process\_attr(): Enter!

187 11/05/2001 14:18:23.600 SEV=9 IKEDBG/1 RPT=66  
Processing cfg ACK attributes

188 11/05/2001 14:18:23.600 SEV=8 IKEDBG/0 RPT=228  
172.18.124.241  
RECEIVED Message (msgid=c06b6315) with payloads :  
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 138

190 11/05/2001 14:18:23.600 SEV=9 IKEDBG/1 RPT=67  
process\_attr(): Enter!

191 11/05/2001 14:18:23.600 SEV=9 IKEDBG/1 RPT=68  
Processing cfg Request attributes

192 11/05/2001 14:18:23.600 SEV=9 IKEDBG/1 RPT=69  
Received IPV4 address request!

193 11/05/2001 14:18:23.600 SEV=9 IKEDBG/1 RPT=70  
Received IPV4 net mask request!

194 11/05/2001 14:18:23.600 SEV=9 IKEDBG/1 RPT=71  
Received DNS server address request!

195 11/05/2001 14:18:23.600 SEV=9 IKEDBG/1 RPT=72  
Received WINS server address request!

196 11/05/2001 14:18:23.600 SEV=6 IKE/130 RPT=3  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Received unsupported transaction mode attribute: 5

198 11/05/2001 14:18:23.600 SEV=6 IKE/130 RPT=4  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]

Received unsupported transaction mode attribute: 7

200 11/05/2001 14:18:23.600 SEV=9 IKEDBG/1 RPT=73  
Received Banner request!

201 11/05/2001 14:18:23.600 SEV=9 IKEDBG/1 RPT=74  
Received Save PW request!

202 11/05/2001 14:18:23.600 SEV=9 IKEDBG/1 RPT=75  
Received Default Domain request!

203 11/05/2001 14:18:23.600 SEV=9 IKEDBG/1 RPT=76  
Received Split Tunnel Include request!

204 11/05/2001 14:18:23.600 SEV=9 IKEDBG/1 RPT=77  
Received PFS request!

205 11/05/2001 14:18:23.600 SEV=9 IKEDBG/1 RPT=78  
Received UDP Port request!

206 11/05/2001 14:18:23.600 SEV=9 IKEDBG/31 RPT=2  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Obtained IP addr (192.168.10.10) prior to initiating  
Mode Cfg (XAuth enabled)

208 11/05/2001 14:18:23.600 SEV=9 IKEDBG/0 RPT=229  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing blank hash

209 11/05/2001 14:18:23.600 SEV=9 IKEDBG/0 RPT=230  
172.18.124.241  
0000: 00010004 C0A80A0A F0010000 F0070000 .....

210 11/05/2001 14:18:23.600 SEV=9 IKEDBG/0 RPT=231  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing qm hash

211 11/05/2001 14:18:23.600 SEV=8 IKEDBG/0 RPT=232  
172.18.124.241  
SENDING Message (msgid=c06b6315) with payloads :  
HDR + HASH (8) ... total length : 72

213 11/05/2001 14:18:23.640 SEV=9 IKEDBG/21 RPT=2  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Delay Quick Mode processing, Cert/Trans Exch/RM  
DSID in progress

215 11/05/2001 14:18:23.640 SEV=4 AUTH/21 RPT=33  
User ipsecuser connected

216 11/05/2001 14:18:23.640 SEV=7 IKEDBG/22 RPT=2  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Resume Quick Mode processing, Cert/Trans Exch/RM  
DSID completed

218 11/05/2001 14:18:23.640 SEV=4 IKE/119 RPT=2  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
PHASE 1 COMPLETED

219 11/05/2001 14:18:23.640 SEV=6 IKE/121 RPT=2  
172.18.124.241  
Keep-alive type for this connection: DPD

220 11/05/2001 14:18:23.640 SEV=7 IKEDBG/0 RPT=233  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Starting phase 1 rekey timer: 73440000 (ms)

221 11/05/2001 14:18:23.640 SEV=9 IKEDBG/0 RPT=234  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
sending notify message

222 11/05/2001 14:18:23.640 SEV=9 IKEDBG/0 RPT=235  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing blank hash

223 11/05/2001 14:18:23.640 SEV=9 IKEDBG/0 RPT=236  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing qm hash

224 11/05/2001 14:18:23.640 SEV=8 IKEDBG/0 RPT=237  
172.18.124.241  
SENDING Message (msgid=2899decd) with payloads :  
HDR + HASH (8) ... total length : 88

226 11/05/2001 14:18:23.640 SEV=8 IKEDBG/0 RPT=238  
172.18.124.241  
RECEIVED Message (msgid=7551d208) with payloads :  
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) +  
ID (5) + NONE (0) ... total leng  
th : 792

229 11/05/2001 14:18:23.640 SEV=9 IKEDBG/0 RPT=239  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
processing hash

230 11/05/2001 14:18:23.640 SEV=9 IKEDBG/0 RPT=240  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
processing SA payload

231 11/05/2001 14:18:23.640 SEV=9 IKEDBG/1 RPT=79  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
processing nonce payload

232 11/05/2001 14:18:23.640 SEV=9 IKEDBG/1 RPT=80  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Processing ID

233 11/05/2001 14:18:23.640 SEV=5 IKE/25 RPT=3  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Received remote Proxy Host data in ID Payload:  
Address 192.168.10.10, Protocol 0, Port 0

236 11/05/2001 14:18:23.640 SEV=9 IKEDBG/1 RPT=81

172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Processing ID

237 11/05/2001 14:18:23.640 SEV=5 IKE/24 RPT=2  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Received local Proxy Host data in ID Payload:  
Address 172.18.124.132, Protocol 0, Port 0

240 11/05/2001 14:18:23.640 SEV=8 IKEDBG/0 RPT=241  
QM IsRekeyed old sa not found by addr

241 11/05/2001 14:18:23.640 SEV=5 IKE/66 RPT=3  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
IKE Remote Peer configured for SA: ESP-3DES-MD5

243 11/05/2001 14:18:23.640 SEV=9 IKEDBG/0 RPT=242  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
processing IPSEC SA

244 11/05/2001 14:18:23.650 SEV=8 IKEDBG/0 RPT=243  
Proposal # 2, Transform # 1, Type ESP, Id Triple-DES  
Parsing received transform:  
Phase 2 failure:  
Mismatched attr types for class HMAC Algorithm:  
Rcv'd: SHA  
Cfg'd: MD5

248 11/05/2001 14:18:23.650 SEV=7 IKEDBG/27 RPT=3  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
IPSec SA Proposal # 3, Transform # 1 acceptable

250 11/05/2001 14:18:23.650 SEV=7 IKEDBG/0 RPT=244  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
IKE: requesting SPI!

251 11/05/2001 14:18:23.650 SEV=9 IPSECDBG/6 RPT=11  
IPSEC key message parse - msgtype 6, len 192, vers 1,  
pid 00000000, seq 3, err 0  
, type 2, mode 0, state 32, label 0, pad 0, spi 00000000,  
encrKeyLen 0, hashKeyL  
en 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1  
7762996, lifetime2 0, dsI  
d 300

255 11/05/2001 14:18:23.650 SEV=9 IPSECDBG/1 RPT=38  
Processing KEY\_GETSPI msg!

256 11/05/2001 14:18:23.650 SEV=7 IPSECDBG/13 RPT=3  
Reserved SPI 1910411637

257 11/05/2001 14:18:23.650 SEV=8 IKEDBG/6 RPT=3  
IKE got SPI from key engine: SPI = 0x71de9175

258 11/05/2001 14:18:23.650 SEV=9 IKEDBG/0 RPT=245  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
oakley constucting quick mode



259 11/05/2001 14:18:23.650 SEV=9 IKEDBG/0 RPT=246  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing blank hash

260 11/05/2001 14:18:23.650 SEV=9 IKEDBG/0 RPT=247  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing ISA\_SA for ipsec

261 11/05/2001 14:18:23.650 SEV=5 IKE/75 RPT=3  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Overriding Initiator's IPSec rekeying duration from  
2147483 to 28800 seconds

263 11/05/2001 14:18:23.650 SEV=9 IKEDBG/1 RPT=82  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing ipsec nonce payload

264 11/05/2001 14:18:23.650 SEV=9 IKEDBG/1 RPT=83  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing proxy ID

265 11/05/2001 14:18:23.650 SEV=7 IKEDBG/0 RPT=248  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Transmitting Proxy Id:  
Remote host: 192.168.10.10 Protocol 0 Port 0  
Local host: 172.18.124.132 Protocol 0 Port 0

269 11/05/2001 14:18:23.650 SEV=7 IKEDBG/0 RPT=249  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Sending RESPONDER LIFETIME notification to Initiator

271 11/05/2001 14:18:23.650 SEV=9 IKEDBG/0 RPT=250  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing qm hash

272 11/05/2001 14:18:23.650 SEV=8 IKEDBG/0 RPT=251 172.18.124.241  
SENDING Message (msgid=7551d208) with payloads :  
HDR + HASH (8) ... total length : 172

274 11/05/2001 14:18:23.650 SEV=8 IKEDBG/0 RPT=252 172.18.124.241  
RECEIVED Message (msgid=6c034bb1) with payloads :  
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) +  
NONE (0) ... total leng  
th : 796

277 11/05/2001 14:18:23.650 SEV=9 IKEDBG/0 RPT=253  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
processing hash

278 11/05/2001 14:18:23.650 SEV=9 IKEDBG/0 RPT=254  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
processing SA payload

279 11/05/2001 14:18:23.650 SEV=9 IKEDBG/1 RPT=84

172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
processing nonce payload

280 11/05/2001 14:18:23.650 SEV=9 IKEDBG/1 RPT=85  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Processing ID

281 11/05/2001 14:18:23.650 SEV=5 IKE/25 RPT=4  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Received remote Proxy Host data in ID Payload:  
Address 192.168.10.10, Protocol 0, Port 0

284 11/05/2001 14:18:23.650 SEV=9 IKEDBG/1 RPT=86  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Processing ID

285 11/05/2001 14:18:23.650 SEV=5 IKE/34 RPT=2  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Received local IP Proxy Subnet data in ID Payload:  
Address 0.0.0.0, Mask 0.0.0.0, Protocol 0, Port 0

288 11/05/2001 14:18:23.650 SEV=8 IKEDBG/0 RPT=255  
QM IsRekeyed old sa not found by addr

289 11/05/2001 14:18:23.650 SEV=5 IKE/66 RPT=4  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
IKE Remote Peer configured for SA: ESP-3DES-MD5

291 11/05/2001 14:18:23.650 SEV=9 IKEDBG/0 RPT=256 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
processing IPSEC SA

292 11/05/2001 14:18:23.660 SEV=8 IKEDBG/0 RPT=257  
Proposal # 2, Transform # 1, Type ESP, Id Triple-DES  
Parsing received transform:  
Phase 2 failure:  
Mismatched attr types for class HMAC Algorithm:  
Rcv'd: SHA  
Cfg'd: MD5

296 11/05/2001 14:18:23.660 SEV=7 IKEDBG/27 RPT=4  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
IPSec SA Proposal # 3, Transform # 1 acceptable

298 11/05/2001 14:18:23.660 SEV=7 IKEDBG/0 RPT=258  
172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
IKE: requesting SPI!

299 11/05/2001 14:18:23.660 SEV=9 IPSECDBG/6 RPT=12  
IPSEC key message parse - msgtype 6, len 192, vers 1,  
pid 00000000, seq 4, err 0, type 2, mode 0, state 32,  
label 0, pad 0, spi 00000000, encrKeyLen 0, hashKeyLen 0,  
ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 7764576,  
lifetime2 0, dsId 300

303 11/05/2001 14:18:23.660 SEV=9 IPSECDBG/1 RPT=39  
Processing KEY\_GETSPI msg!

304 11/05/2001 14:18:23.660 SEV=7 IPSECDBG/13 RPT=4  
Reserved SPI 1940396912

305 11/05/2001 14:18:23.660 SEV=8 IKEDBG/6 RPT=4  
IKE got SPI from key engine: SPI = 0x73a81b70

306 11/05/2001 14:18:23.660 SEV=9 IKEDBG/0 RPT=259 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
oakley constructing quick mode

307 11/05/2001 14:18:23.660 SEV=9 IKEDBG/0 RPT=260 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing blank hash

308 11/05/2001 14:18:23.660 SEV=9 IKEDBG/0 RPT=261 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing ISA\_SA for ipsec

309 11/05/2001 14:18:23.660 SEV=5 IKE/75 RPT=4 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Overriding Initiator's IPsec rekeying duration from  
2147483 to 28800 seconds

311 11/05/2001 14:18:23.660 SEV=9 IKEDBG/1 RPT=87 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing ipsec nonce payload

312 11/05/2001 14:18:23.660 SEV=9 IKEDBG/1 RPT=88 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing proxy ID

313 11/05/2001 14:18:23.660 SEV=7 IKEDBG/0 RPT=262 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Transmitting Proxy Id:  
Remote host: 192.168.10.10 Protocol 0 Port 0  
Local subnet: 0.0.0.0 mask 0.0.0.0 Protocol 0 Port 0

317 11/05/2001 14:18:23.660 SEV=7 IKEDBG/0 RPT=263 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Sending RESPONDER LIFETIME notification to Initiator

319 11/05/2001 14:18:23.660 SEV=9 IKEDBG/0 RPT=264 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
constructing qm hash

320 11/05/2001 14:18:23.660 SEV=8 IKEDBG/0 RPT=265 172.18.124.241  
SENDING Message (msgid=6c034bb1) with payloads :  
HDR + HASH (8) ... total length : 176

322 11/05/2001 14:18:23.660 SEV=8 IKEDBG/0 RPT=266 172.18.124.241  
RECEIVED Message (msgid=7551d208) with payloads :  
HDR + HASH (8) + NONE (0) ... total length : 48

324 11/05/2001 14:18:23.660 SEV=9 IKEDBG/0 RPT=267 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
processing hash

325 11/05/2001 14:18:23.660 SEV=9 IKEDBG/0 RPT=268 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
loading all IPSEC SAs

326 11/05/2001 14:18:23.660 SEV=9 IKEDBG/1 RPT=89 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Generating Quick Mode Key!

327 11/05/2001 14:18:23.660 SEV=9 IKEDBG/1 RPT=90 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Generating Quick Mode Key!

328 11/05/2001 14:18:23.670 SEV=7 IKEDBG/0 RPT=269 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Loading host:  
Dst: 172.18.124.132  
Src: 192.168.10.10

330 11/05/2001 14:18:23.670 SEV=4 IKE/49 RPT=3 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Security negotiation complete for User (ipsecuser)  
Responder, Inbound SPI = 0x71de9175, Outbound SPI = 0x2081f1c4

333 11/05/2001 14:18:23.670 SEV=9 IPSECDBG/6 RPT=13  
IPSEC key message parse - msgtype 1, len 608, vers 1,  
pid 00000000, seq 0, err 0, type 2, mode 1, state 64,  
label 0, pad 0, spi 2081f1c4, encrKeyLen 24, hashKeyLen 16,  
ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 7764576,  
lifetime2 0, dsId 0

337 11/05/2001 14:18:23.670 SEV=9 IPSECDBG/1 RPT=40  
Processing KEY\_ADD msg!

338 11/05/2001 14:18:23.670 SEV=9 IPSECDBG/1 RPT=41  
key\_msghdr2secassoc(): Enter

339 11/05/2001 14:18:23.670 SEV=7 IPSECDBG/1 RPT=42  
No USER filter configured

340 11/05/2001 14:18:23.670 SEV=9 IPSECDBG/1 RPT=43  
KeyProcessAdd: Enter

341 11/05/2001 14:18:23.670 SEV=8 IPSECDBG/1 RPT=44  
KeyProcessAdd: Adding outbound SA

342 11/05/2001 14:18:23.670 SEV=8 IPSECDBG/1 RPT=45  
KeyProcessAdd: src 172.18.124.132 mask 0.0.0.0, dst  
192.168.10.10 mask 0.0.0.0

343 11/05/2001 14:18:23.670 SEV=8 IPSECDBG/1 RPT=46  
KeyProcessAdd: FilterIpsecAddIkeSa success

344 11/05/2001 14:18:23.670 SEV=9 IPSECDBG/6 RPT=14  
IPSEC key message parse - msgtype 3, len 328, vers 1,  
pid 00000000, seq 0, err 0, type 2, mode 1, state 32,  
label 0, pad 0, spi 71de9175, encrKeyLen 24, hashKeyLen 16,  
ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 7762996,  
lifetime2 0, dsId 0

348 11/05/2001 14:18:23.670 SEV=9 IPSECDBG/1 RPT=47  
Processing KEY\_UPDATE msg!

349 11/05/2001 14:18:23.670 SEV=9 IPSECDBG/1 RPT=48  
Update inbound SA addresses

350 11/05/2001 14:18:23.670 SEV=9 IPSECDBG/1 RPT=49  
key\_msghdr2secassoc(): Enter

351 11/05/2001 14:18:23.670 SEV=7 IPSECDBG/1 RPT=50  
No USER filter configured

352 11/05/2001 14:18:23.670 SEV=9 IPSECDBG/1 RPT=51  
KeyProcessUpdate: Enter

353 11/05/2001 14:18:23.670 SEV=8 IPSECDBG/1 RPT=52  
KeyProcessUpdate: success

354 11/05/2001 14:18:23.670 SEV=8 IKEDBG/7 RPT=3  
IKE got a KEY\_ADD msg for SA: SPI = 0x2081f1c4

355 11/05/2001 14:18:23.670 SEV=8 IKEDBG/0 RPT=270  
pitcher: rcv KEY\_UPDATE, spi 0x71de9175

356 11/05/2001 14:18:23.670 SEV=4 IKE/120 RPT=3 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
PHASE 2 COMPLETED (msgid=7551d208)

357 11/05/2001 14:18:23.690 SEV=8 IKEDBG/0 RPT=271 172.18.124.241  
RECEIVED Message (msgid=6c034bb1) with payloads :  
HDR + HASH (8) + NONE (0) ... total length : 48

359 11/05/2001 14:18:23.690 SEV=9 IKEDBG/0 RPT=272 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
processing hash

360 11/05/2001 14:18:23.690 SEV=9 IKEDBG/0 RPT=273 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
loading all IPSEC SAs

361 11/05/2001 14:18:23.690 SEV=9 IKEDBG/1 RPT=91 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Generating Quick Mode Key!

362 11/05/2001 14:18:23.690 SEV=9 IKEDBG/1 RPT=92 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Generating Quick Mode Key!

363 11/05/2001 14:18:23.690 SEV=7 IKEDBG/0 RPT=274 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Loading subnet:  
Dst: 0.0.0.0 mask: 0.0.0.0  
Src: 192.168.10.10

365 11/05/2001 14:18:23.690 SEV=4 IKE/49 RPT=4 172.18.124.241  
Group [ipsecgroup] User [ipsecuser]  
Security negotiation complete for User (ipsecuser)  
Responder, Inbound SPI = 0x73a81b70, Outbound SPI = 0xaf8534c2

368 11/05/2001 14:18:23.690 SEV=9 IPSECDBG/6 RPT=15  
IPSEC key message parse - msgtype 1, len 608, vers 1,  
pid 00000000, seq 0, err 0, type 2, mode 1, state 64,  
label 0, pad 0, spi af8534c2, encrKeyLen 24, hashKeyLen 16,  
ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 7764576,  
lifetime2 0, dsId 0

372 11/05/2001 14:18:23.690 SEV=9 IPSECDBG/1 RPT=53  
Processing KEY\_ADD msg!

373 11/05/2001 14:18:23.690 SEV=9 IPSECDBG/1 RPT=54  
key\_msghdr2secassoc(): Enter

374 11/05/2001 14:18:23.690 SEV=7 IPSECDBG/1 RPT=55

```
No USER filter configured

375 11/05/2001 14:18:23.690 SEV=9 IPSECDBG/1 RPT=56
KeyProcessAdd: Enter

376 11/05/2001 14:18:23.690 SEV=8 IPSECDBG/1 RPT=57
KeyProcessAdd: Adding outbound SA

377 11/05/2001 14:18:23.690 SEV=8 IPSECDBG/1 RPT=58
KeyProcessAdd: src 0.0.0.0 mask 255.255.255.255, dst
192.168.10.10 mask 0.0.0.0

378 11/05/2001 14:18:23.690 SEV=8 IPSECDBG/1 RPT=59
KeyProcessAdd: FilterIpsecAddIkeSa success

379 11/05/2001 14:18:23.690 SEV=9 IPSECDBG/6 RPT=16
IPSEC key message parse - msgtype 3, len 328, vers 1,
pid 00000000, seq 0, err 0, type 2, mode 1, state 32,
label 0, pad 0, spi 73a81b70, encrKeyLen 24, hashKeyLen 16,
ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 7762996,
lifetime2 0, dsId 0

383 11/05/2001 14:18:23.690 SEV=9 IPSECDBG/1 RPT=60
Processing KEY_UPDATE msg!

384 11/05/2001 14:18:23.690 SEV=9 IPSECDBG/1 RPT=61
Update inbound SA addresses

385 11/05/2001 14:18:23.690 SEV=9 IPSECDBG/1 RPT=62
key_msghdr2secassoc(): Enter

386 11/05/2001 14:18:23.690 SEV=7 IPSECDBG/1 RPT=63
No USER filter configured

387 11/05/2001 14:18:23.690 SEV=9 IPSECDBG/1 RPT=64
KeyProcessUpdate: Enter

388 11/05/2001 14:18:23.690 SEV=8 IPSECDBG/1 RPT=65
KeyProcessUpdate: success

389 11/05/2001 14:18:23.690 SEV=8 IKEDBG/7 RPT=4
IKE got a KEY_ADD msg for SA: SPI = 0xaf8534c2

390 11/05/2001 14:18:23.690 SEV=8 IKEDBG/0 RPT=275
pitcher: rcv KEY_UPDATE, spi 0x73a81b70

391 11/05/2001 14:18:23.690 SEV=4 IKE/120 RPT=4 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
PHASE 2 COMPLETED (msgid=6c034bb1)
```

## Causes de problèmes potentiels

- [Impossible de négocier IPSec ou l'hôte ne répond pas](#)
- [L'utilisateur ne peut pas se connecter](#)
- [Aucun débogage de concentrateur VPN 3000 et aucun utilisateur ne peut se connecter](#)

## Impossible de négocier IPSec ou l'hôte ne répond pas

Le débogage du concentrateur VPN 3000 présente les éléments suivants :

14 02/20/2001 08:59:29.100 SEV=4 IKE/22 RPT=5 64.102.55.139  
No Group found matching badgroup for Pre-shared key peer 64.102.55.139

La cause habituelle de ce problème est que l'utilisateur tente de se connecter avec un nom de groupe qui n'est pas configuré.

### L'utilisateur ne peut pas se connecter

Il y a plusieurs problèmes possibles si vous ne pouvez pas vous connecter.

- **Filtre manquant**Le débogage du concentrateur VPN 3000 présente les éléments suivants :  
Filter missing on interface 2, IKE data from Peer x.x.x.x dropped  
La cause habituelle de ce problème est que le filtre est absent de l'interface publique. Il devrait généralement être le filtre public (mais peut être le filtre privé ; « aucun » n'est valide). Accédez à **Configuration > Interfaces > Ethernet 2 > Filter** et définissez le filtre « public » ou une autre valeur (qui n'est pas « aucun »).
- **IPSec non sélectionné**Le message d'erreur est le suivant :  
Unable to negotiate IPSec or host did not respond.

Le débogage du concentrateur VPN 3000 présente les éléments suivants :

Terminating connection attempt: IPSEC not permitted for group <group>

La cause habituelle de ce problème est qu'IPSec n'est pas sélectionné sur le groupe.

Accédez à **Configuration > User Management > Groups ><group> Modify > General tab** et vérifiez que IPSec est sélectionné sous Tunneling Protocols.

- **Utilisateur non dans la base de données**Le message d'erreur est le suivant :  
User Authentication Failed

Le débogage du concentrateur VPN 3000 présente les éléments suivants :

Authentication rejected: Reason = User was not found handle = 14,  
server = Internal, user = <user>

La cause habituelle de ce problème est que l'utilisateur n'existe pas dans la base de données utilisateur. Assurez-vous que vous saisissez le nom d'utilisateur correct lorsque l'écran d'authentification de l'utilisateur s'affiche.

- **Route par défaut manquante**Le débogage du concentrateur VPN 3000 présente les éléments suivants :  
Filter missing on interface 0, IKE data from Peer x.x.x.x dropped

La cause habituelle de ce problème est que la route par défaut est manquante. Assurez-vous qu'il existe une route par défaut dans la configuration. Accédez à **Configuration > System > IP routing > Default Gateway** pour spécifier la passerelle par défaut.

- **Aucune option d'adresse IP**Le message d'erreur est le suivant :  
Your IPSec connection has been terminated by the remote peer.

Le débogage du concentrateur VPN 3000 présente les éléments suivants :

User [ >user< ]

IKE rcv'd FAILED IP Addr status!

La cause habituelle de ce problème est qu'aucune option n'est cochée pour donner une adresse IP au client. Accédez à **Configuration > System > Address Management > Address Assignment** pour sélectionner une option.

- **Mots de passe différents** Le message d'erreur est le suivant :

```
User authentication failed
```

Le débogage du concentrateur VPN 3000 présente les éléments suivants :

```
The calculated HASH doesn't match the received value
```

La cause habituelle de ce problème est que le mot de passe de groupe sur le client est différent du mot de passe configuré sur le concentrateur. Vérifiez les mots de passe sur le client et le concentrateur.

### [Aucun débogage de concentrateur VPN 3000 et aucun utilisateur ne peut se connecter](#)

Le filtre public du concentrateur par défaut contient des règles permettant le trafic suivant :

```
Protocol = UDP, port = 500  
Protocol = UDP, port = 10000  
Protocol = ESP  
Protocol = AH
```

Si les filtres du concentrateur VPN 3000 autorisent ce trafic, alors un périphérique entre le client et le concentrateur peut bloquer certains de ces ports (peut-être un pare-feu). Pour vérifier, essayez de vous connecter au concentrateur à partir du réseau immédiatement en dehors du concentrateur. Si cela fonctionne, un périphérique entre le PC client et le concentrateur bloque le trafic.

## [Informations connexes](#)

- [Page d'assistance du concentrateur VPN Cisco 3000](#)
- [Cisco VPN Client Support Page](#)
- [Page d'assistance IPsec](#)
- [Téléchargement du logiciel du client VPN](#)
- [Support et documentation techniques - Cisco Systems](#)