# Configuring IPSec from VPN Client Version 3.5 Solaris to a VPN 3000 Concentrator

## Índice



## Introdução

Este documento ilustra como configurar o cliente VPN 3.5 para Solaris 2.6 para conectar a um VPN 3000 concentrator.

## Pré-requisitos

### Requisitos

Antes de tentar utilizar esta configuração, verifique se os seguintes pré-requisitos são atendidos.

- Este exemplo usa a chave pré-compartilhada para a autenticação do grupo. O nome de usuário e senha (autenticação extendida) é verificado contra o base de dados interno do concentrador VPN.
- O cliente VPN deve corretamente ser instalado. Refira a instalação do cliente VPN para Solaris para detalhes na instalação.
- A conectividade IP deve existir entre o cliente VPN e a interface pública do concentrador VPN. A máscara de sub-rede e a informação de gateway devem ser ajustadas corretamente.

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware.

- Cisco VPN Client para a versão 3.5 de Solaris 2.6, imagem 3DES. (nome da imagem: vpnclient-solaris5.6-3.5.Rel-k9.tar.Z)
- Tipo do Cisco VPN concentrator: Rev do código de inicialização 3005: Altiga Networks/VPN versão do concentrador 2.2.int_9 Rev do software do 19 de janeiro de 2000 05:36:41: Cisco Systems, Inc. /VPN 3000 Concentrator Series versão 3.1.Rel do 6 de agosto de 2001 13:47:37

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

### Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

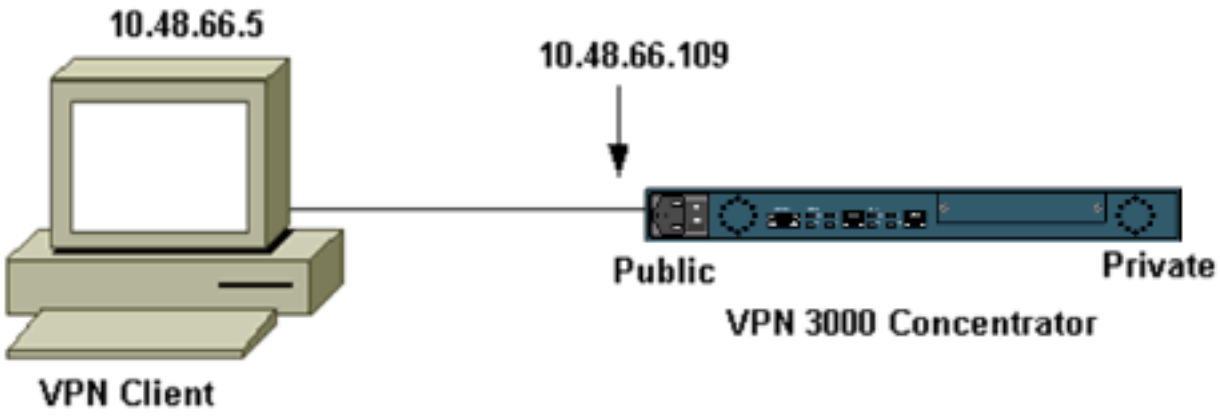
## Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

**Nota:** Para localizar informações adicionais sobre os comandos usados neste documento, utilize a Ferramenta Command Lookup (somente clientes registrados).

### Diagrama de Rede

Este documento utiliza a instalação de rede mostrada no diagrama abaixo.




**Nota:** Para o cliente VPN 3.5 a conectar ao concentrador VPN, você precisa a versão 3.0 ou mais tarde o concentrador.

### Configurações

#### Criando um perfil de usuário para a conexão

Os perfis de usuário são armazenados no diretório de /etc/CiscoSystemsVPNClient/Profiles. Estes arquivos de texto têm uma extensão do .pcf e contêm os parâmetros necessários

estabeleceram uma conexão a um concentrador VPN. Você pode criar um arquivo novo ou editar existente. Você deve encontrar um exemplo de perfil, sample.pcf, no diretório do perfil. Este exemplo segue o uso desse arquivo criar um perfil novo nomeado toCORPORATE.pcf.

```
[cholera]: ~ > cd /etc/CiscoSystemsVPNClient/Profiles/
[cholera]: /etc/CiscoSystemsVPNClient/Profiles > cp sample.pcf toCORPORATE.pcf
```

Você pode usar seu editor de texto favorito para editar este arquivo novo, toCORPORATE.pcf. Antes de todas as alterações, o arquivo olha como o seguinte.

**Nota:** Se você quer usar o IPsec sobre o Network Address Translation (NAT), a entrada EnableNat na configuração abaixo deve dizer "EnableNat=1" em vez de "EnableNat=0."

```
[main]
Description=sample user profile
Host=10.7.44.1
AuthType=1
GroupName=monkeys
EnableISPConnect=0
ISPConnectType=0
ISPConnect=
ISPCommand=
Username=chimchim
SaveUserPassword=0
EnableBackup=0
BackupServer=
EnableNat=0
CertStore=0
CertName=
CertPath=
CertSubjectName=
CertSerialHash=00000000000000000000000000000000
DHGroup=2
ForceKeepAlives=0
```

Consulte perfis do toUser para uma descrição das palavras-chaves do perfil de usuário.

Para configurar com sucesso seu perfil, você precisa de conhecer, como um mínimo, seus valores equivalentes para a informação seguinte.

- O nome de host ou o endereço IP público do concentrador VPN (10.48.66.109)
- O nome do grupo (RemoteClient)
- O group password (Cisco)
- O username (Joe)

Edite o arquivo com sua informação de modo que seja similar ao seguinte.

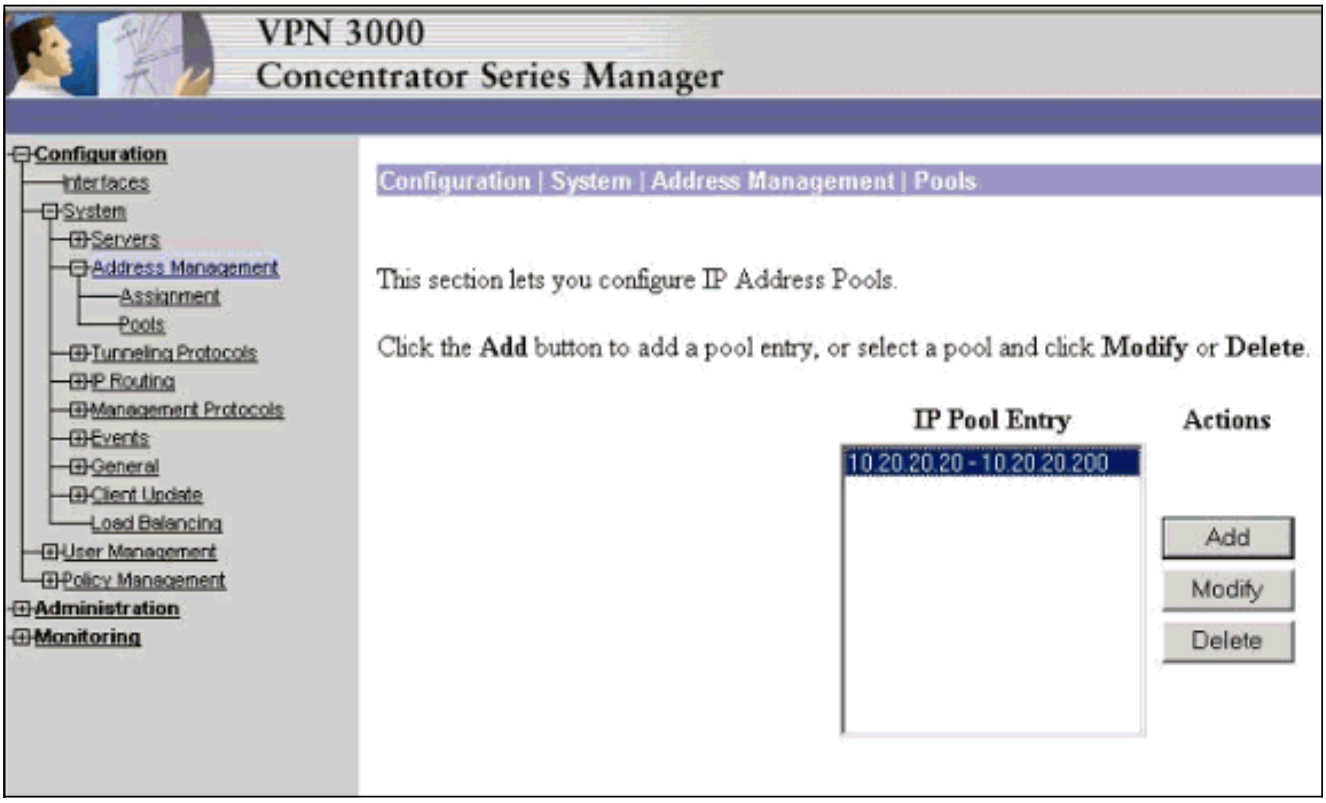
```
[main]
Description=Connection to the corporate
Host=10.48.66.109 AuthType=1 GroupName=RemoteClient GroupPwd=cisco EnableISPConnect=0
ISPConnectType=0 ISPConnect= ISPCommand= Username=joe SaveUserPassword=0 EnableBackup=0
BackupServer= EnableNat=0 CertStore=0 CertName= CertPath= CertSubjectName=
CertSerialHash=00000000000000000000000000000000 DHGroup=2 ForceKeepAlives=0
```

## Configurando o concentrador de VPN

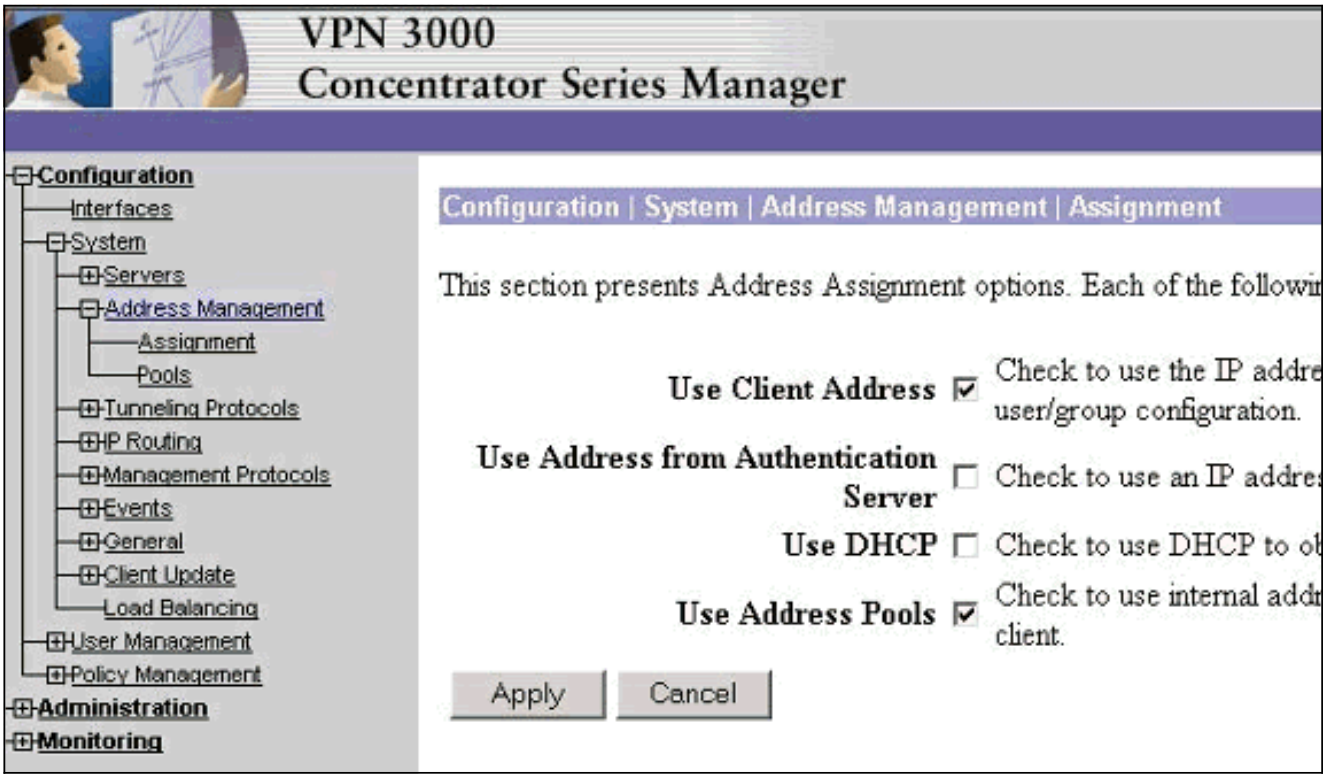
Use as seguintes etapas para configurar o concentrador VPN.

**Nota:** Devido às limitações de espaço, as capturas de tela mostram somente parcial ou áreas relevantes.

1. Atribua o conjunto de endereço. Para atribuir uma escala disponível dos endereços IP de Um ou Mais Servidores Cisco ICM NT, aponte um navegador à interface interna do concentrador VPN e selecione **>Pools do configuração > sistema > gerenciamento de endereço**. Clique em Add. Especifique uma faixa de endereços IP que não entrem em conflito com nenhum outro dispositivo na rede interna.

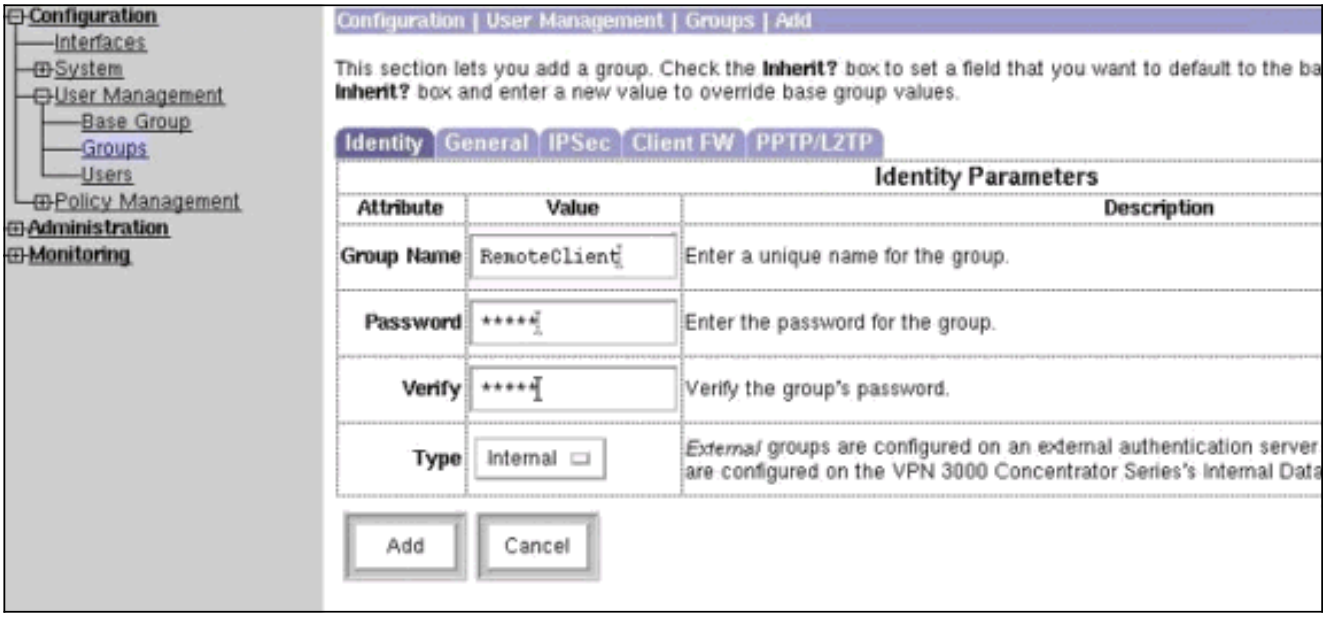



2. Para dizer o concentrador VPN para usar o pool, o **configuração > sistema > gerenciamento de endereço > atribuição** seleto, verifica a caixa dos **conjuntos de endereços do uso**, e clica-a então **aplica-se**.

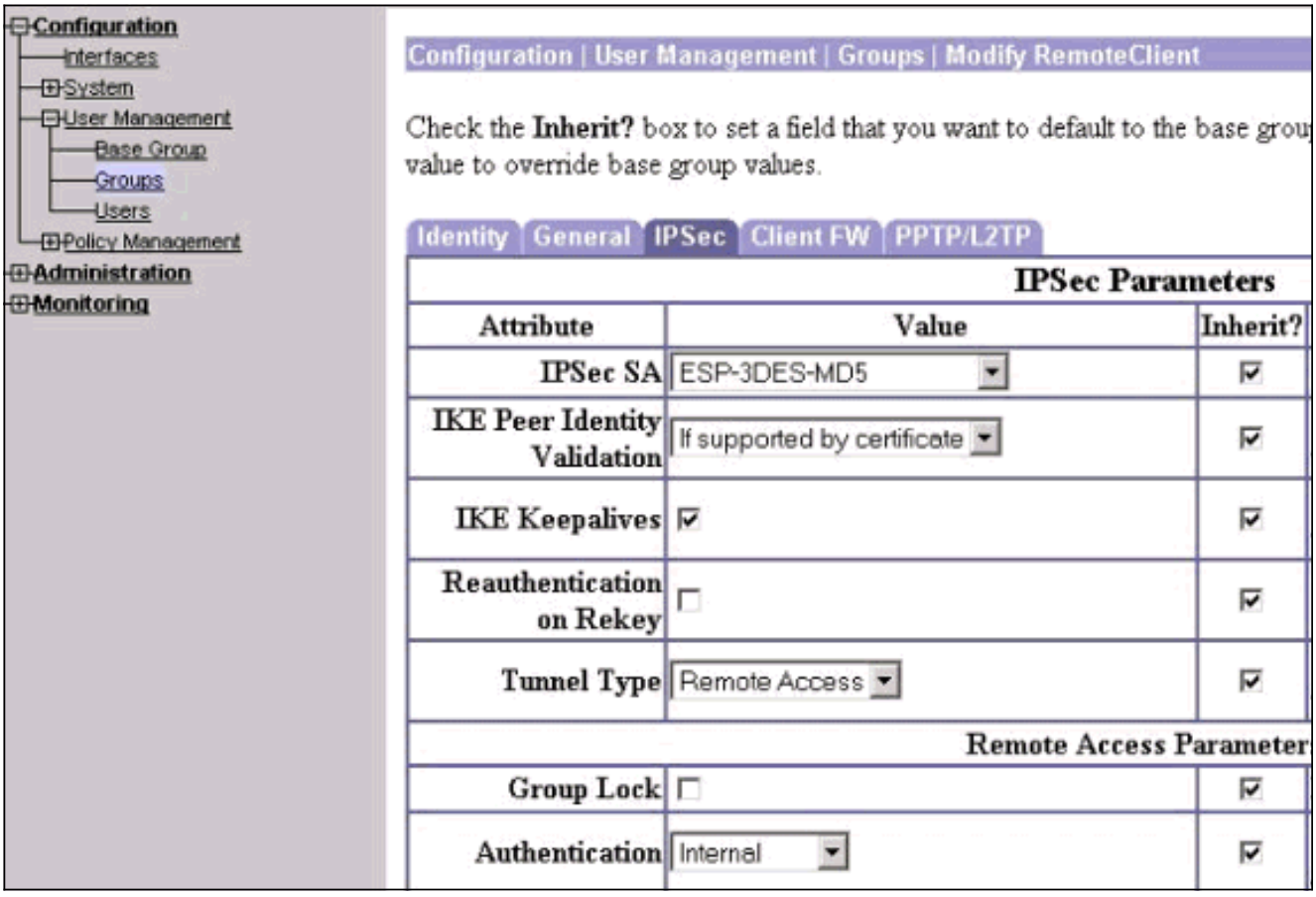



3. Adicionar um grupo e uma senha. Selecione o **configuration > user management > os**

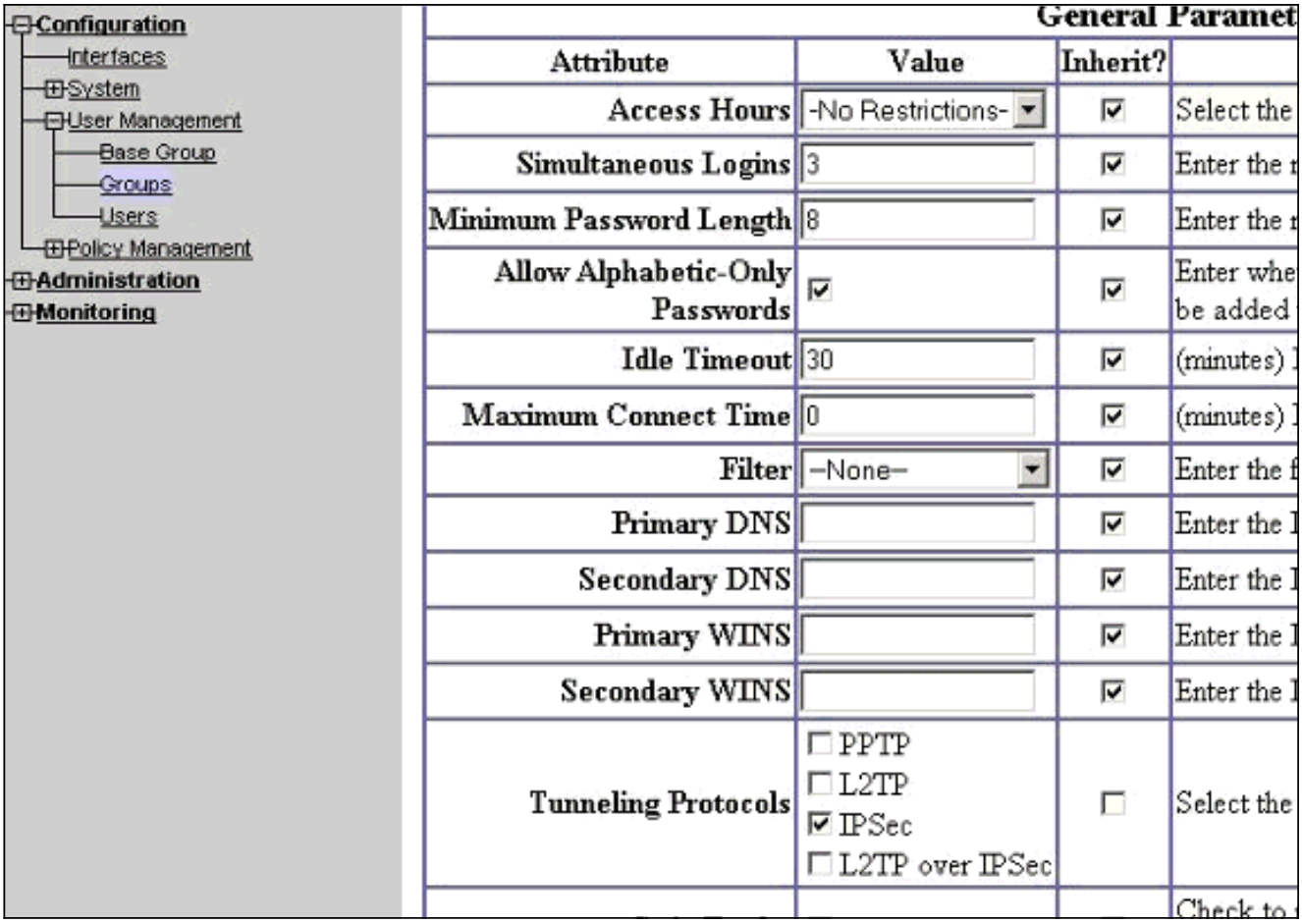
**grupos**, e clique-os então **adicionam o grupo**. Incorpore a informação correta, e clique-a então **adicionam** para submeter a informação.Este exemplo usa um grupo nomeado “RemoteClient” com uma senha de
“Cisco.”



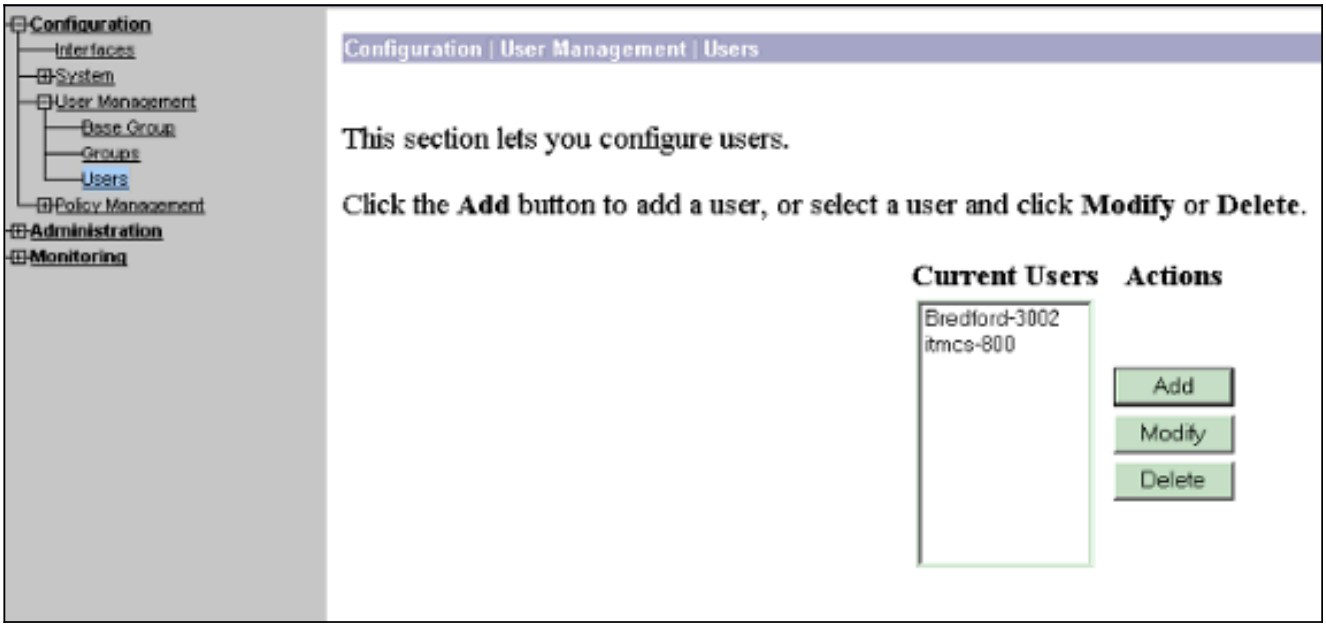

4. Na aba do IPsec do grupo, verifica que a autenticação está ajustada a **interno**.



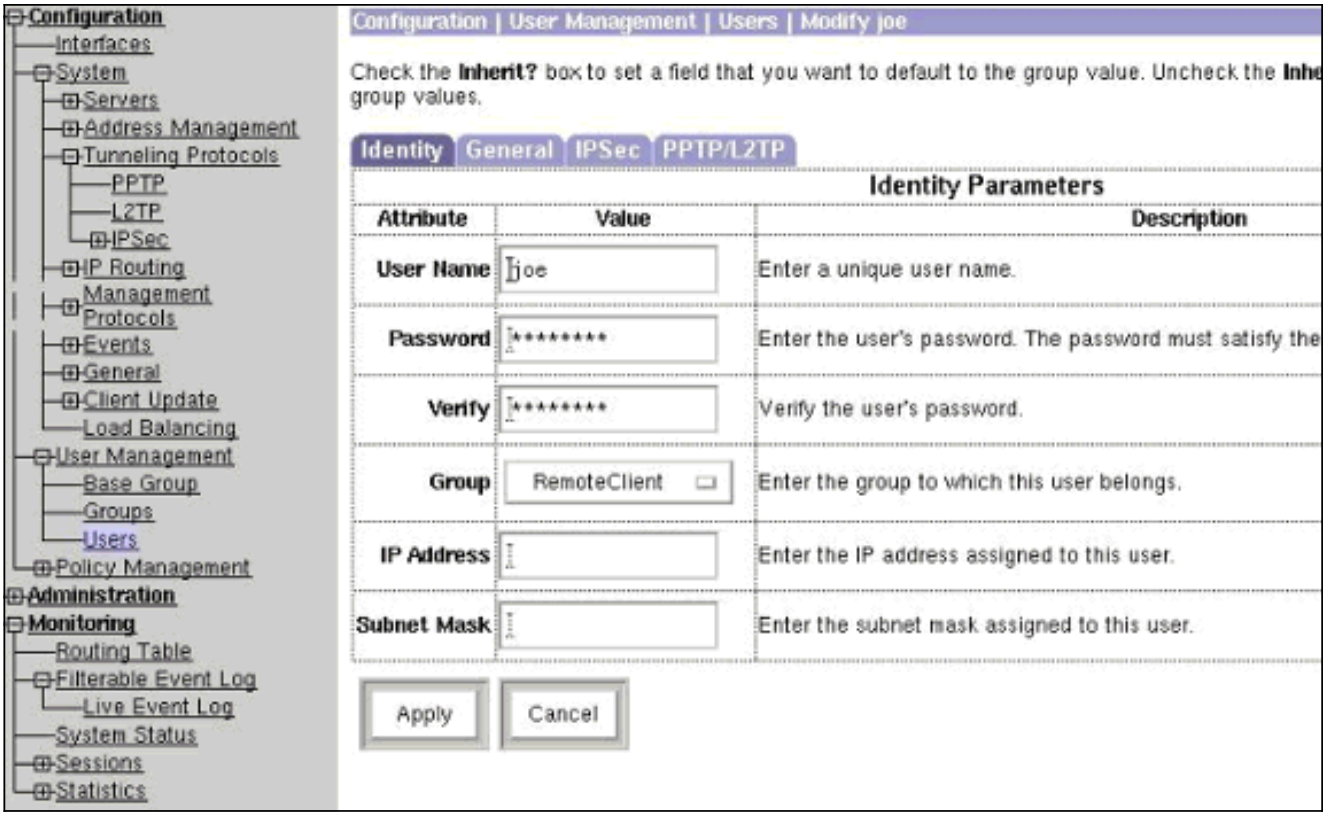

5. No tab geral do grupo, verifique que o **IPsec** está selecionado como os protocolos de tunelamento.




6. Para adicionar o usuário ao concentrador VPN, o **configuration > user management** seleto **> os usuários**, e clicá-lo então **adicionam**.




7. Incorpore a informação correta para o grupo, e clique-a então **aplica-se** para submeter a informação.




# Verificar

## Conectando ao concentrador de VPN

Agora que o cliente VPN e o concentrador são configurados, o perfil novo deve trabalhar para conectar ao concentrador VPN.

```
91 [cholera]: /etc/CiscoSystemsVPNClient > vpnclient connect toCORPORATE Cisco Systems VPN
Client Version 3.5 (Rel) Copyright (C) 1998-2001 Cisco Systems, Inc. All Rights Reserved. Client
Type(s): Solaris Running on: SunOS 5.6 Generic_105181-11 sun4u Initializing the IPSec link.
Contacting the security gateway at 10.48.66.109 Authenticating user. User Authentication for
toCORPORATE... Enter Username and Password. Username [Joe]: Password []: Contacting the security
gateway at 10.48.66.109 Your link is secure. IPSec tunnel information. Client address:
10.20.20.20 Server address: 10.48.66.109 Encryption: 168-bit 3-DES Authentication: HMAC-MD5 IP
Compression: None NAT passthrough is inactive. Local LAN Access is disabled. ^Z Suspended
[cholera]: /etc/CiscoSystemsVPNClient > bg [1] vpnclient connect toCORPORATE & (The process is
made to run as background process) [cholera]: /etc/CiscoSystemsVPNClient > vpnclient disconnect
Cisco Systems VPN Client Version 3.5 (Rel) Copyright (C) 1998-2001 Cisco Systems, Inc. All
Rights Reserved. Client Type(s): Solaris Running on: SunOS 5.6 Generic_105181-11 sun4u Your
IPSec link has been disconnected. Disconnecting the IPSEC link. [cholera]:
/etc/CiscoSystemsVPNClient > [1] Exit -56 vpnclient connect toCORPORATE [cholera]:
/etc/CiscoSystemsVPNClient >
```

# Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

## Debugs

Para permitir debuga, usam o **comando ipseclog**. Um exemplo é mostrado abaixo.

[cholera]: /etc/CiscoSystemsVPNClient > **ipseclog /tmp/clientlog**

## Debugar no cliente ao conectar ao concentrador

[cholera]: /etc/CiscoSystemsVPNClient > **cat /tmp/clientlog** 1 17:08:49.821 01/25/2002 Sev=Info/4 CLI/0x43900002 Started vpnclient: Cisco Systems VPN Client Version 3.5 (Rel) Copyright (C) 1998-2001 Cisco Systems, Inc. All Rights Reserved. Client Type(s): Solaris Running on: SunOS 5.6 Generic_105181-11 sun4u 2 17:08:49.855 01/25/2002 Sev=Info/4 CVPND/0x4340000F Started cvpnd: Cisco Systems VPN Client Version 3.5 (Rel) Copyright (C) 1998-2001 Cisco Systems, Inc. All Rights Reserved. Client Type(s): Solaris Running on: SunOS 5.6 Generic_105181-11 sun4u 3 17:08:49.857 01/25/2002 Sev=Info/4 IPSEC/0x43700013 Delete internal key with SPI=0xb0f0d0c0 4 17:08:49.857 01/25/2002 Sev=Info/4 IPSEC/0x4370000C Key deleted by SPI 0xb0f0d0c0 5 17:08:49.858 01/25/2002 Sev=Info/4 IPSEC/0x43700013 Delete internal key with SPI=0x637377d3 6 17:08:49.858 01/25/2002 Sev=Info/4 IPSEC/0x4370000C Key deleted by SPI 0x637377d3 7 17:08:49.859 01/25/2002 Sev=Info/4 IPSEC/0x43700013 Delete internal key with SPI=0x9d4d2b9d 8 17:08:49.859 01/25/2002 Sev=Info/4 IPSEC/0x4370000C Key deleted by SPI 0x9d4d2b9d 9 17:08:49.859 01/25/2002 Sev=Info/4 IPSEC/0x43700013 Delete internal key with SPI=0x5facd5bf 10 17:08:49.860 01/25/2002 Sev=Info/4 IPSEC/0x4370000C Key deleted by SPI 0x5facd5bf 11 17:08:49.860 01/25/2002 Sev=Info/4 IPSEC/0x43700009 IPSec driver already started 12 17:08:49.861 01/25/2002 Sev=Info/4 IPSEC/0x43700014 Deleted all keys 13 17:08:49.861 01/25/2002 Sev=Info/4 IPSEC/0x43700014 Deleted all keys 14 17:08:49.862 01/25/2002 Sev=Info/4 IPSEC/0x43700009 IPSec driver already started 15 17:08:49.863 01/25/2002 Sev=Info/4 IPSEC/0x43700009 IPSec driver already started 16 17:08:49.863 01/25/2002 Sev=Info/4 IPSEC/0x43700014 Deleted all keys 17 17:08:50.873 01/25/2002 Sev=Info/4 CM/0x43100002 Begin connection process 18 17:08:50.883 01/25/2002 Sev=Info/4 CM/0x43100004 Establish secure connection using Ethernet 19 17:08:50.883 01/25/2002 Sev=Info/4 CM/0x43100026 Attempt connection with server "10.48.66.109" 20 17:08:50.883 01/25/2002 Sev=Info/6 IKE/0x4300003B Attempting to establish a connection with 10.48.66.109. 21 17:08:51.099 01/25/2002 Sev=Info/4 IKE/0x43000013 SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID) to 10.48.66.109 22 17:08:51.099 01/25/2002 Sev=Info/4 IPSEC/0x43700009 IPSec driver already started 23 17:08:51.100 01/25/2002 Sev=Info/4 IPSEC/0x43700014 Deleted all keys 24 17:08:51.400 01/25/2002 Sev=Info/5 IKE/0x4300002F Received ISAKMP packet: peer = 10.48.66.109 25 17:08:51.400 01/25/2002 Sev=Info/4 IKE/0x43000014 RECEIVING <<< ISAKMP OAK AG (SA, KE, NON, ID, HASH, VID, VID, VID, VID) from 10.48.66.109 26 17:08:51.400 01/25/2002 Sev=Info/5 IKE/0x43000059 Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100 27 17:08:51.400 01/25/2002 Sev=Info/5 IKE/0x43000001 Peer is a Cisco-Unity compliant peer 28 17:08:51.400 01/25/2002 Sev=Info/5 IKE/0x43000059 Vendor ID payload = 09002689DFD6B712 29 17:08:51.400 01/25/2002 Sev=Info/5 IKE/0x43000059 Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100 30 17:08:51.400 01/25/2002 Sev=Info/5 IKE/0x43000001 Peer supports DPD 31 17:08:51.400 01/25/2002 Sev=Info/5 IKE/0x43000059 Vendor ID payload = 1F07F70EAA6514D3B0FA96542A500301 32 17:08:51.505 01/25/2002 Sev=Info/4 IKE/0x43000013 SENDING >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT) to 10.48.66.109 33 17:08:51.510 01/25/2002 Sev=Info/5 IKE/0x4300002F Received ISAKMP packet: peer = 10.48.66.109 34 17:08:51.511 01/25/2002 Sev=Info/4 IKE/0x43000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 10.48.66.109 35 17:08:51.511 01/25/2002 Sev=Info/4 CM/0x43100015 Launch xAuth application 36 17:08:56.333 01/25/2002 Sev=Info/4 CM/0x43100017 xAuth application returned 37 17:08:56.334 01/25/2002 Sev=Info/4 IKE/0x43000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 10.48.66.109 38 17:08:56.636 01/25/2002 Sev=Info/5 IKE/0x4300002F Received ISAKMP packet: peer = 10.48.66.109 39 17:08:56.637 01/25/2002 Sev=Info/4 IKE/0x43000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 10.48.66.109 40 17:08:56.637 01/25/2002 Sev=Info/4 CM/0x4310000E Established Phase 1 SA. 1 Phase 1 SA in the system 41 17:08:56.639 01/25/2002 Sev=Info/4 IKE/0x43000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 10.48.66.109 42 17:08:56.639 01/25/2002 Sev=Info/4 IKE/0x43000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 10.48.66.109 43 17:08:56.645 01/25/2002 Sev=Info/5 IKE/0x4300002F Received ISAKMP packet: peer = 10.48.66.109 44 17:08:56.646 01/25/2002 Sev=Info/4 IKE/0x43000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 10.48.66.109 45 17:08:56.646 01/25/2002 Sev=Info/5 IKE/0x43000010 MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: , value = 10.20.20.20 46 17:08:56.646 01/25/2002 Sev=Info/5 IKE/0x4300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value = 0x00000000 47 17:08:56.646 01/25/2002 Sev=Info/5 IKE/0x4300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_PFS: , value = 0x00000000 48 17:08:56.646 01/25/2002 Sev=Info/5 IKE/0x4300000E MODE_CFG_REPLY: Attribute = APPLICATION_VERSION, value = Cisco Systems, Inc./VPN 3000 Concentrator Series Version 3.1.Rel built by vmurphy on Aug 06 2001 13:47:37 49 17:08:56.648 01/25/2002 Sev=Info/4 CM/0x43100019 Mode Config data received 50 17:08:56.651 01/25/2002 Sev=Info/5 IKE/0x43000055 Received a key request from Driver for IP address 10.48.66.109, GW IP = 10.48.66.109 51 17:08:56.652 01/25/2002 Sev=Info/4 IKE/0x43000013 SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID,

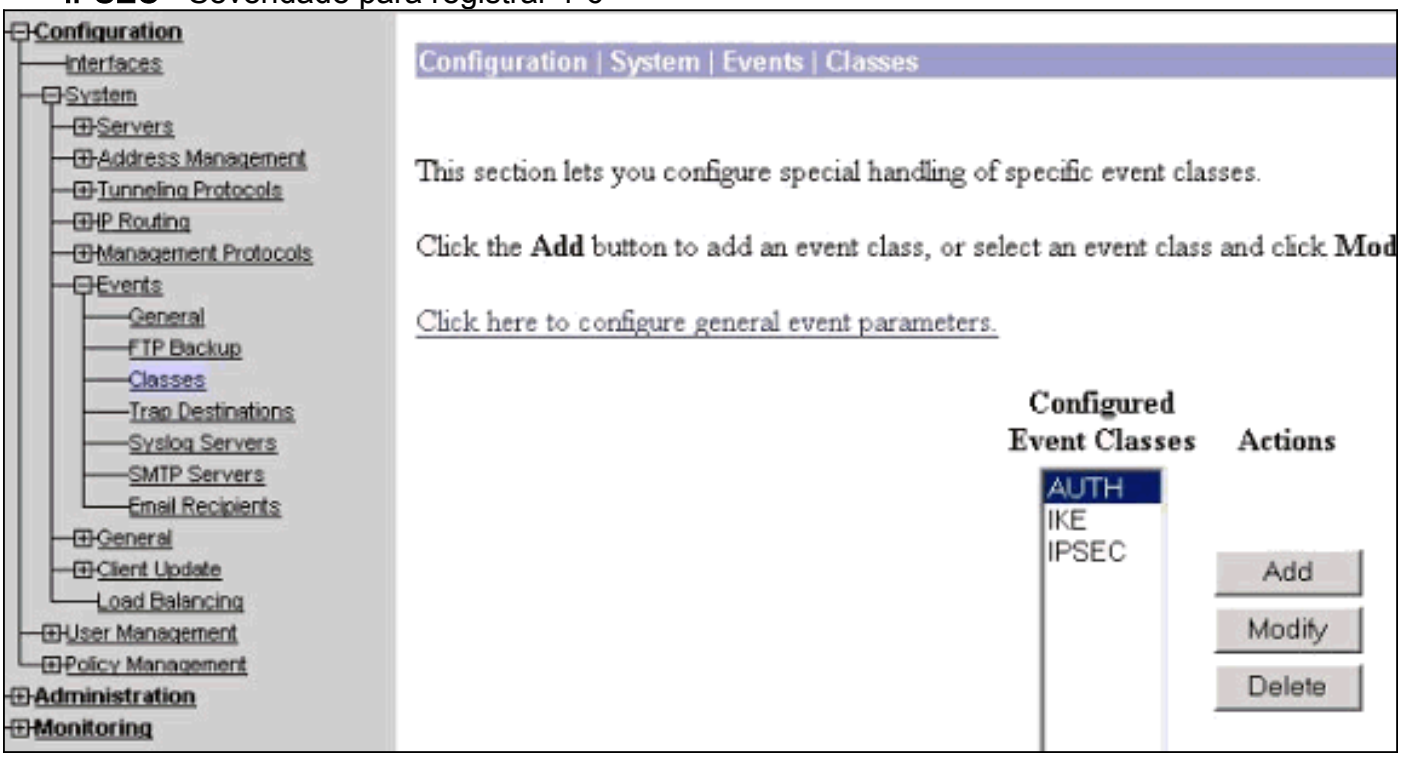
ID) to 10.48.66.109 52 17:08:56.653 01/25/2002 Sev=Info/5 IKE/0x43000055 Received a key request from Driver for IP address 10.10.10.255, GW IP = 10.48.66.109 53 17:08:56.653 01/25/2002 Sev=Info/4 IKE/0x43000013 SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 10.48.66.109 54 17:08:56.663 01/25/2002 Sev=Info/5 IKE/0x4300002F Received ISAKMP packet: peer = 10.48.66.109 55 17:08:56.663 01/25/2002 Sev=Info/4 IKE/0x43000014 RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:STATUS_RESP_LIFETIME) from 10.48.66.109 56 17:08:56.663 01/25/2002 Sev=Info/5 IKE/0x43000044 RESPONDER-LIFETIME notify has value of 86400 seconds 57 17:08:56.663 01/25/2002 Sev=Info/5 IKE/0x43000046 This SA has already been alive for 6 seconds, setting expiry to 86394 seconds from now 58 17:08:56.666 01/25/2002 Sev=Info/5 IKE/0x4300002F Received ISAKMP packet: peer = 10.48.66.109 59 17:08:56.666 01/25/2002 Sev=Info/4 IKE/0x43000014 RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME) from 10.48.66.109 60 17:08:56.667 01/25/2002 Sev=Info/5 IKE/0x43000044 RESPONDER-LIFETIME notify has value of 28800 seconds 61 17:08:56.667 01/25/2002 Sev=Info/4 IKE/0x43000013 SENDING >>> ISAKMP OAK QM *(HASH) to 10.48.66.109 62 17:08:56.667 01/25/2002 Sev=Info/5 IKE/0x43000058 Loading IPsec SA (Message ID = 0x4CEF4B32 OUTBOUND SPI = 0x5EAD41F5 INBOUND SPI = 0xE66C759A) 63 17:08:56.668 01/25/2002 Sev=Info/5 IKE/0x43000025 Loaded OUTBOUND ESP SPI: 0x5EAD41F5 64 17:08:56.669 01/25/2002 Sev=Info/5 IKE/0x43000026 Loaded INBOUND ESP SPI: 0xE66C759A 65 17:08:56.669 01/25/2002 Sev=Info/4 CM/0x4310001A One secure connection established 66 17:08:56.674 01/25/2002 Sev=Info/5 IKE/0x4300002F Received ISAKMP packet: peer = 10.48.66.109 67 17:08:56.675 01/25/2002 Sev=Info/4 IKE/0x43000014 RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME) from 10.48.66.109 68 17:08:56.675 01/25/2002 Sev=Info/5 IKE/0x43000044 RESPONDER-LIFETIME notify has value of 28800 seconds 69 17:08:56.675 01/25/2002 Sev=Info/4 IKE/0x43000013 SENDING >>> ISAKMP OAK QM *(HASH) to 10.48.66.109 70 17:08:56.675 01/25/2002 Sev=Info/5 IKE/0x43000058 Loading IPsec SA (Message ID = 0x88E9321A OUTBOUND SPI = 0x333B4239 INBOUND SPI = 0x6B040746) 71 17:08:56.677 01/25/2002 Sev=Info/5 IKE/0x43000025 Loaded OUTBOUND ESP SPI: 0x333B4239 72 17:08:56.677 01/25/2002 Sev=Info/5 IKE/0x43000026 Loaded INBOUND ESP SPI: 0x6B040746 73 17:08:56.678 01/25/2002 Sev=Info/4 CM/0x43100022 Additional Phase 2 SA established. 74 17:08:57.752 01/25/2002 Sev=Info/4 IPSEC/0x43700014 Deleted all keys 75 17:08:57.752 01/25/2002 Sev=Info/4 IPSEC/0x43700010 Created a new key structure 76 17:08:57.752 01/25/2002 Sev=Info/4 IPSEC/0x4370000F Added key with SPI=0x5ead41f5 into key list 77 17:08:57.753 01/25/2002 Sev=Info/4 IPSEC/0x43700010 Created a new key structure 78 17:08:57.753 01/25/2002 Sev=Info/4 IPSEC/0x4370000F Added key with SPI=0xe66c759a into key list 79 17:08:57.754 01/25/2002 Sev=Info/4 IPSEC/0x43700010 Created a new key structure 80 17:08:57.754 01/25/2002 Sev=Info/4 IPSEC/0x4370000F Added key with SPI=0x333b4239 into key list 81 17:08:57.754 01/25/2002 Sev=Info/4 IPSEC/0x43700010 Created a new key structure 82 17:08:57.755 01/25/2002 Sev=Info/4 IPSEC/0x4370000F Added key with SPI=0x6b040746 into key list 83 17:09:13.752 01/25/2002 Sev=Info/6 IKE/0x4300003D Sending DPD request to 10.48.66.109, seq# = 2948297981 84 17:09:13.752 01/25/2002 Sev=Info/4 IKE/0x43000013 SENDING >>> ISAKMP OAK INFO *(HASH, NOTIFY:DPD_REQUEST) to 10.48.66.109 85 17:09:13.758 01/25/2002 Sev=Info/5 IKE/0x4300002F Received ISAKMP packet: peer = 10.48.66.109 86 17:09:13.758 01/25/2002 Sev=Info/4 IKE/0x43000014 RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:DPD_ACK) from 10.48.66.109 87 17:09:13.759 01/25/2002 Sev=Info/5 IKE/0x4300003F Received DPD ACK from 10.48.66.109, seq# received = 2948297981, seq# expected = 2948297981 debug on the client when disconnecting 88 17:09:16.366 01/25/2002 Sev=Info/4 CLI/0x43900002 Started vpnclient: Cisco Systems VPN Client Version 3.5 (Rel) Copyright (C) 1998-2001 Cisco Systems, Inc. All Rights Reserved. Client Type(s): Solaris Running on: SunOS 5.6 Generic_105181-11 sun4u 89 17:09:16.367 01/25/2002 Sev=Info/4 CM/0x4310000A Secure connections terminated 90 17:09:16.367 01/25/2002 Sev=Info/5 IKE/0x43000018 Deleting IPsec SA: (OUTBOUND SPI = 333B4239 INBOUND SPI = 6B040746) 91 17:09:16.368 01/25/2002 Sev=Info/4 IKE/0x43000013 SENDING >>> ISAKMP OAK INFO *(HASH, DEL) to 10.48.66.109 92 17:09:16.369 01/25/2002 Sev=Info/5 IKE/0x43000018 Deleting IPsec SA: (OUTBOUND SPI = 5EAD41F5 INBOUND SPI = E66C759A) 93 17:09:16.369 01/25/2002 Sev=Info/4 IKE/0x43000013 SENDING >>> ISAKMP OAK INFO *(HASH, DEL) to 10.48.66.109 94 17:09:16.370 01/25/2002 Sev=Info/4 IKE/0x43000013 SENDING >>> ISAKMP OAK INFO *(HASH, DEL) to 10.48.66.109 95 17:09:16.371 01/25/2002 Sev=Info/4 CM/0x43100013 Phase 1 SA deleted cause by DEL_REASON_RESET_SADB. 0 Phase 1 SA currently in the system 96 17:09:16.371 01/25/2002 Sev=Info/5 CM/0x43100029 Initializing CVPNDrv 97 17:09:16.371 01/25/2002 Sev=Info/6 CM/0x43100035 Tunnel to headend device 10.48.66.109 disconnected: duration: 0 days 0:0:20 98 17:09:16.375 01/25/2002 Sev=Info/5 CM/0x43100029 Initializing CVPNDrv 99 17:09:16.377 01/25/2002 Sev=Info/5 IKE/0x4300002F Received ISAKMP packet: peer = 10.48.66.109 100 17:09:16.377 01/25/2002 Sev=Warning/2 IKE/0x83000061 Attempted incoming connection from 10.48.66.109. Inbound connections are not allowed. 101 17:09:17.372 01/25/2002 Sev=Info/4 IPSEC/0x43700013 Delete internal key with SPI=0x6b040746 102 17:09:17.372 01/25/2002 Sev=Info/4 IPSEC/0x43700013 Delete internal key with SPI=0x333b4239 103 17:09:17.373 01/25/2002 Sev=Info/4 IPSEC/0x43700013 Delete internal key with SPI=0xe66c759a 104 17:09:17.373 01/25/2002 Sev=Info/4 IPSEC/0x43700013 Delete internal key with SPI=0x5ead41f5 105 17:09:17.373 01/25/2002 Sev=Info/4 IPSEC/0x43700014 Deleted

```
all keys 106 17:09:17.374 01/25/2002 Sev=Info/4 IPSEC/0x43700009 IPSec driver already started
107 17:09:17.374 01/25/2002 Sev=Info/4 IPSEC/0x43700014 Deleted all keys 108 17:09:17.375
01/25/2002 Sev=Info/4 IPSEC/0x43700009 IPSec driver already started 109 17:09:17.375 01/25/2002
Sev=Info/4 IPSEC/0x43700014 Deleted all keys 110 17:09:17.375 01/25/2002 Sev=Info/4
IPSEC/0x43700009 IPSec driver already started 111 17:09:17.376 01/25/2002 Sev=Info/4
IPSEC/0x43700014 Deleted all keys
```

[Debuga no concentrador VPN]

**O configuração > sistema > eventos > classes** seleto para girar sobre o seguinte debuga se há umas falhas da conexão dos eventos.

- **AUTH** - Severidade para registrar 1-13
- **IKE** - Severidade para registrar 1-6
- **IPSEC** - Severidade para registrar 1-6




Você pode ver o log selecionando a **monitoração > o log de eventos**.

# Informações Relacionadas

- Página de suporte do Cisco VPN 3000 Series Concentrator
- Página de suporte ao cliente do Cisco VPN 3000 Series
- Página de suporte do IPSec
- Suporte Técnico - Cisco Systems