Configurando um Cisco VPN 5000 Concentrator com autenticação externa para um servidor RADIUS de IAS do Microsoft Windows 2000.

Índice

Introdução

Este documento descreve os procedimentos usados para configurar um concentrador do Cisco VPN 5000 com autenticação externa a um Internet Authentication Server do Microsoft Windows 2000 (IAS) com RAIO.

Note: O protocolo de autenticação de cumprimento do desafio (RACHADURA) não trabalha. Use somente o protocolo password authentication (PAP). Refira a identificação de bug Cisco CSCdt96941 (clientes registrados somente) para uns detalhes mais adicionais.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações aqui são baseadas nesta versão de software:

- Versão de software do concentrador 6.0.16.0001 do Cisco VPN 5000

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 a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

Configuração do concentrador Cisco VPN 5000

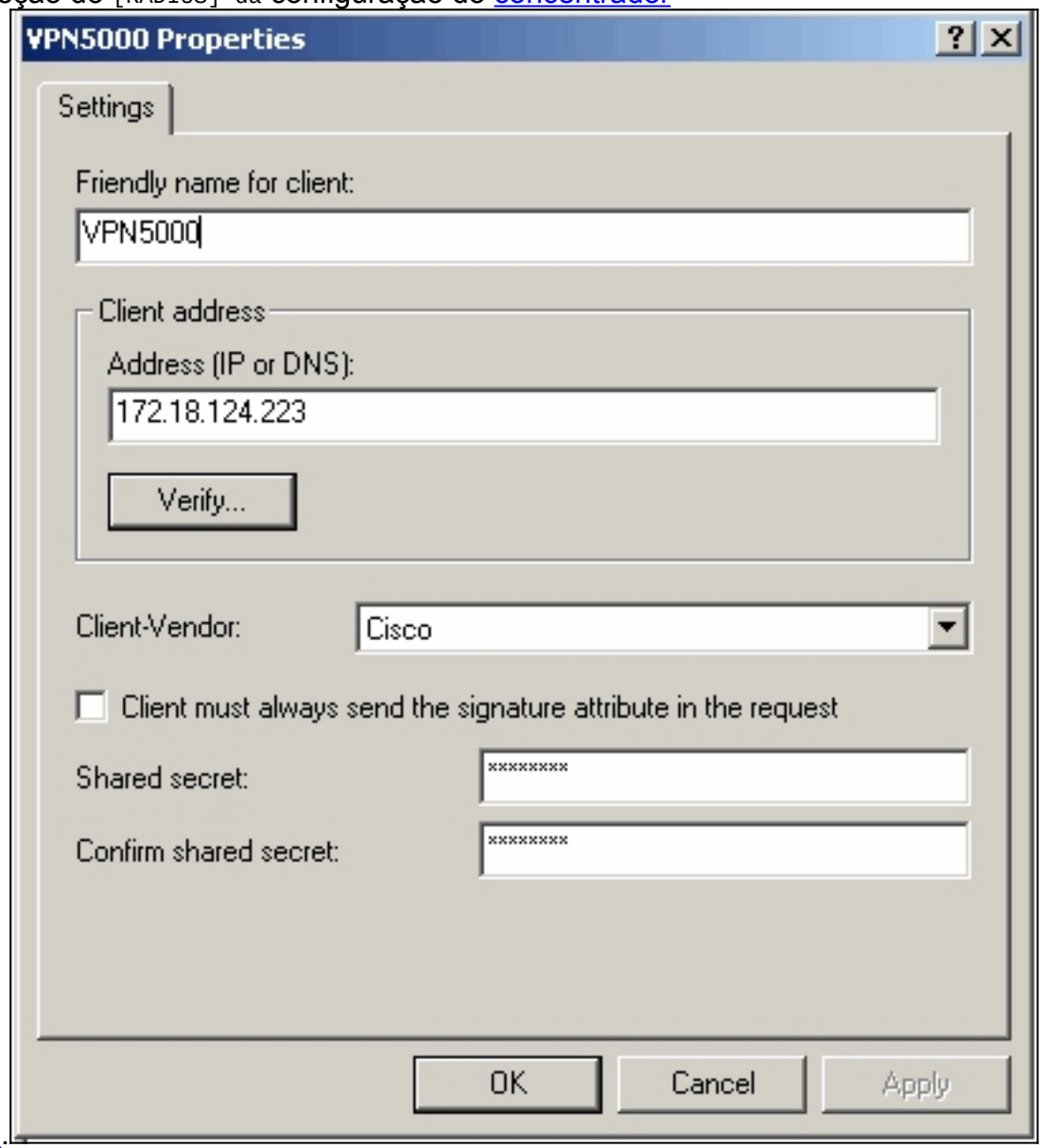
VPN5001_4B9CBA80

```
VPN5001_4B9CBA80> show config
Enter Password:

Edited Configuration not Present, using Running

[ General ]
EthernetAddress          = 00:02:4b:9c:ba:80
DeviceType               = VPN 5001 Concentrator
ConfiguredOn             = Timeserver not configured
ConfiguredFrom           = Command Line, from Console
EnablePassword           =
Password                 =

[ IP Ethernet 0 ]
Mode                     = Routed
SubnetMask               = 255.255.255.0
IPAddress                = 172.18.124.223

[ IP Ethernet 1 ]
Mode                     = Off

[ IKE Policy ]
Protection               = MD5_DES_G1

[ VPN Group "rtp-group" ]
BindTo                   = "ethernet0"
Transform                = esp(md5,des)
LocalIPNet               = 10.1.1.0/24
MaxConnections           = 10
IPNet                    = 0.0.0.0/0

[ RADIUS ]
BindTo                   = "ethernet0"
ChallengeType            = PAP
PAPAuthSecret            = "pappassword"
PrimAddress              = "172.18.124.108"
Secret                   = "radiuspassword"
UseChap16                = Off
Authentication           = On

[ Logging ]
Level                    = 7
Enabled                  = On

Configuration size is 1065 out of 65500 bytes.
VPN5001_4B9CBA80#
```

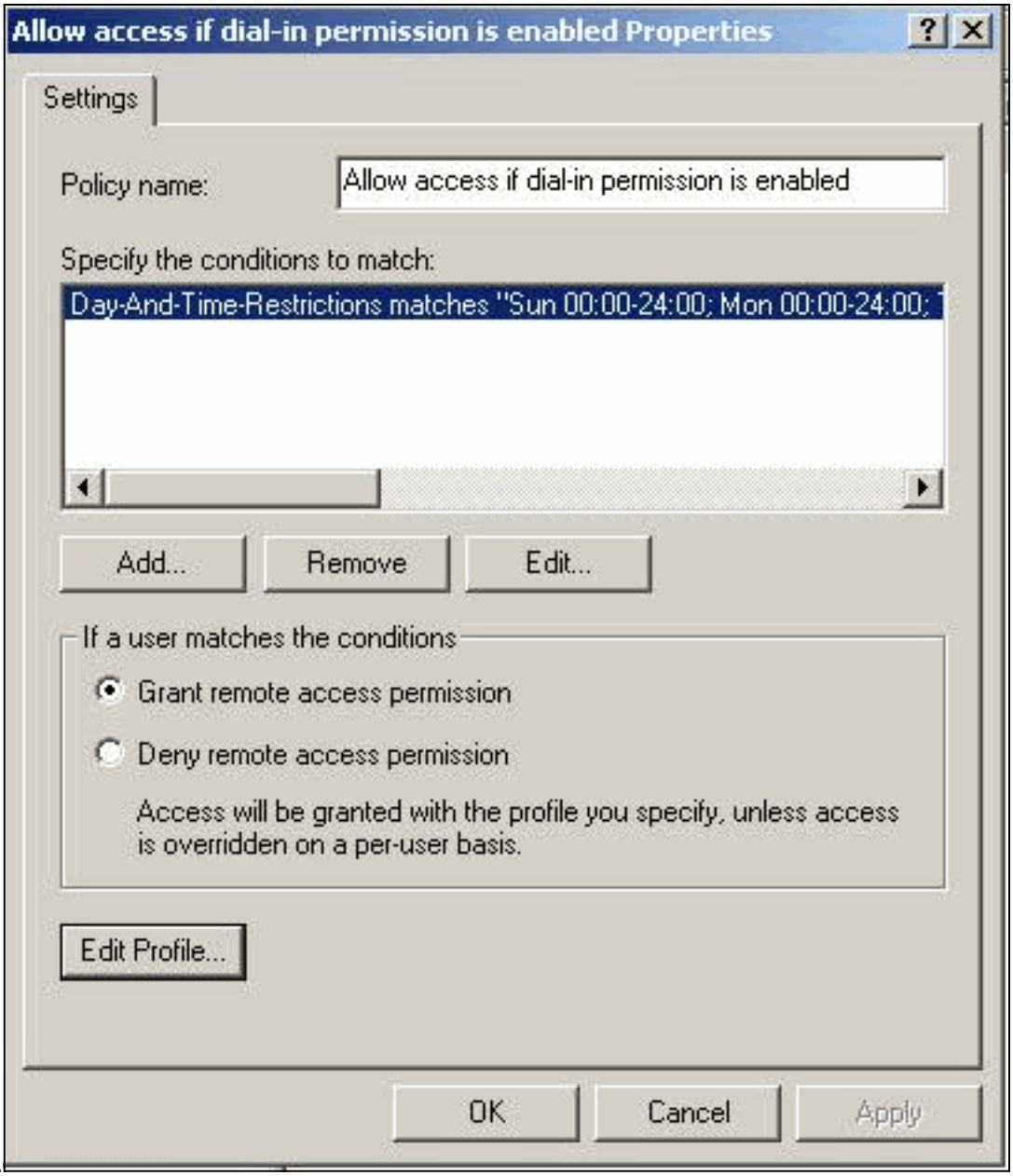
Configurar o servidor Radius de IAS do Microsoft Windows 2000

Estas etapas guiam-no com uma configuração de servidor RADIUS simples de IAS do Microsoft Windows 2000.

1. Sob as propriedades IAS do Microsoft Windows 2000, os **clientes** seletos e criam um cliente novo.Neste exemplo, uma entrada nomeada VPN5000 é criada. O endereço IP de Um ou Mais Servidores Cisco ICM NT do concentrador do Cisco VPN 5000 é 172.18.124.223. Sob a caixa suspensa de Client-Vendor, selecione **Cisco**. O segredo compartilhado é o segredo na seção do `[RADIUS] da` configuração do concentrador VPN.

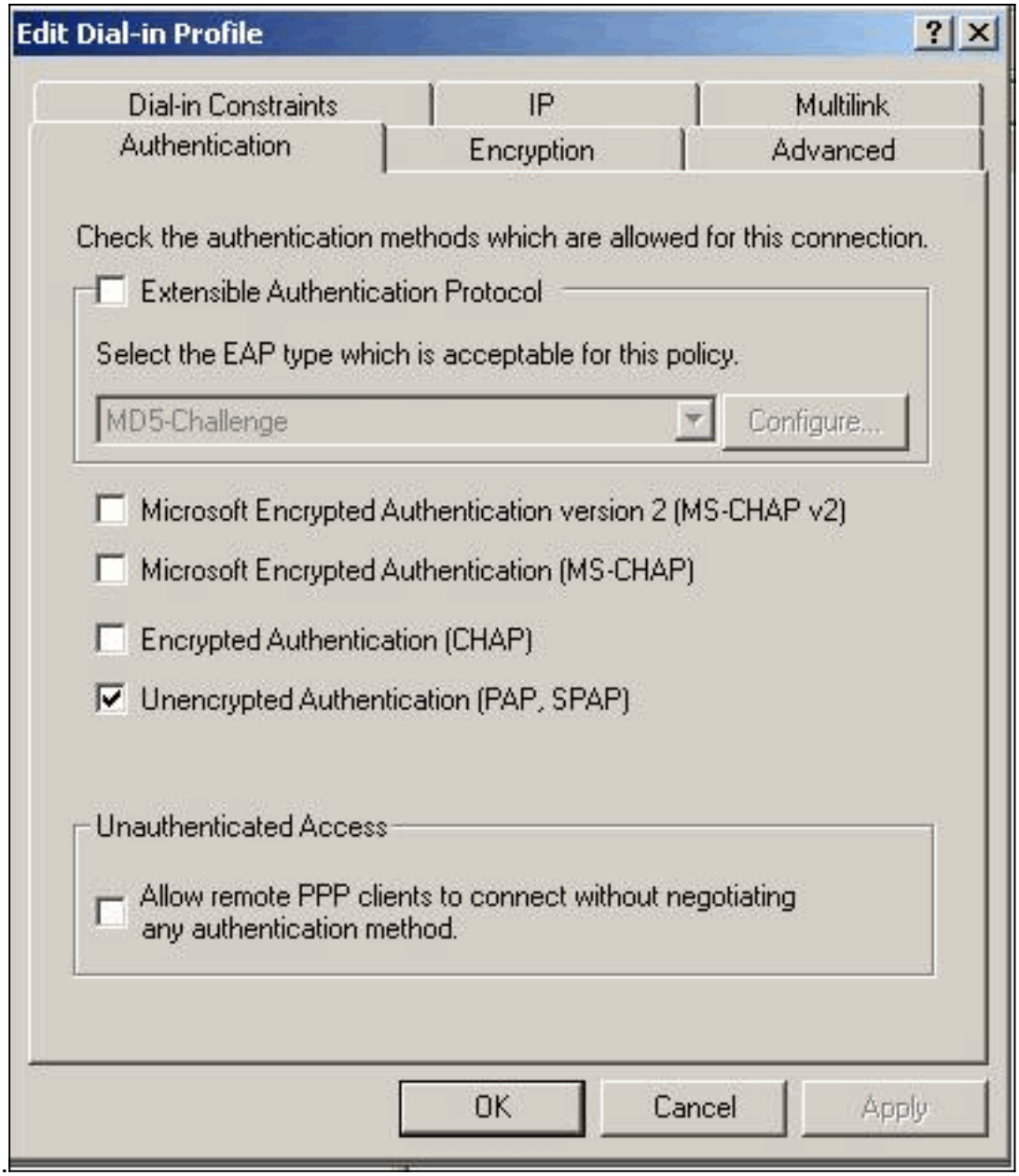


2. Sob as propriedades da política de acesso remoto, selecione **Grant que a permissão de acesso remoto** sob “se um usuário combina as circunstâncias” seção e as clica então **edita o**



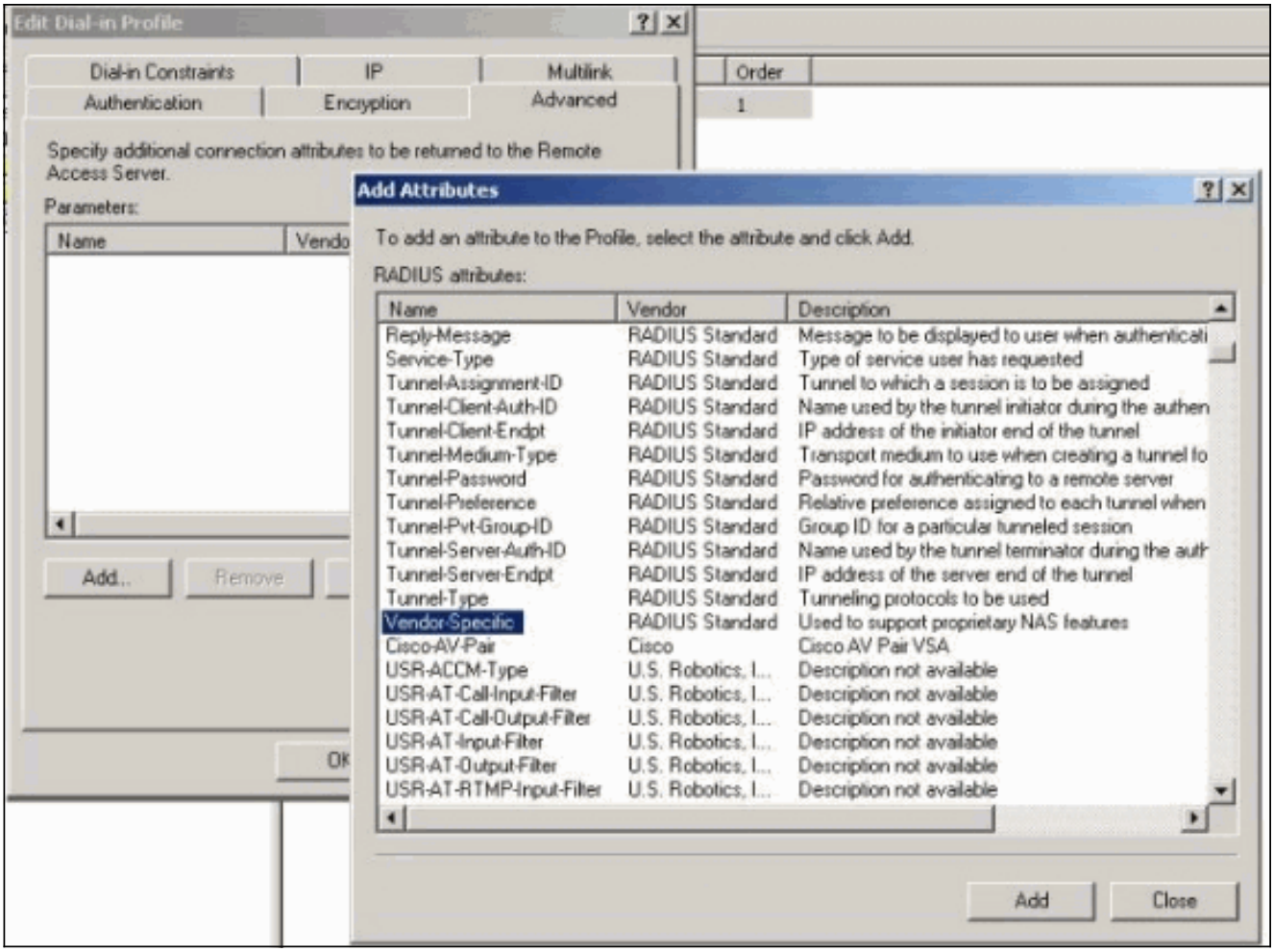
perfil.

3. Clique a aba da autenticação e assegure-se de que essa somente **autenticação não criptografada (PAP, SPAP)** esteja

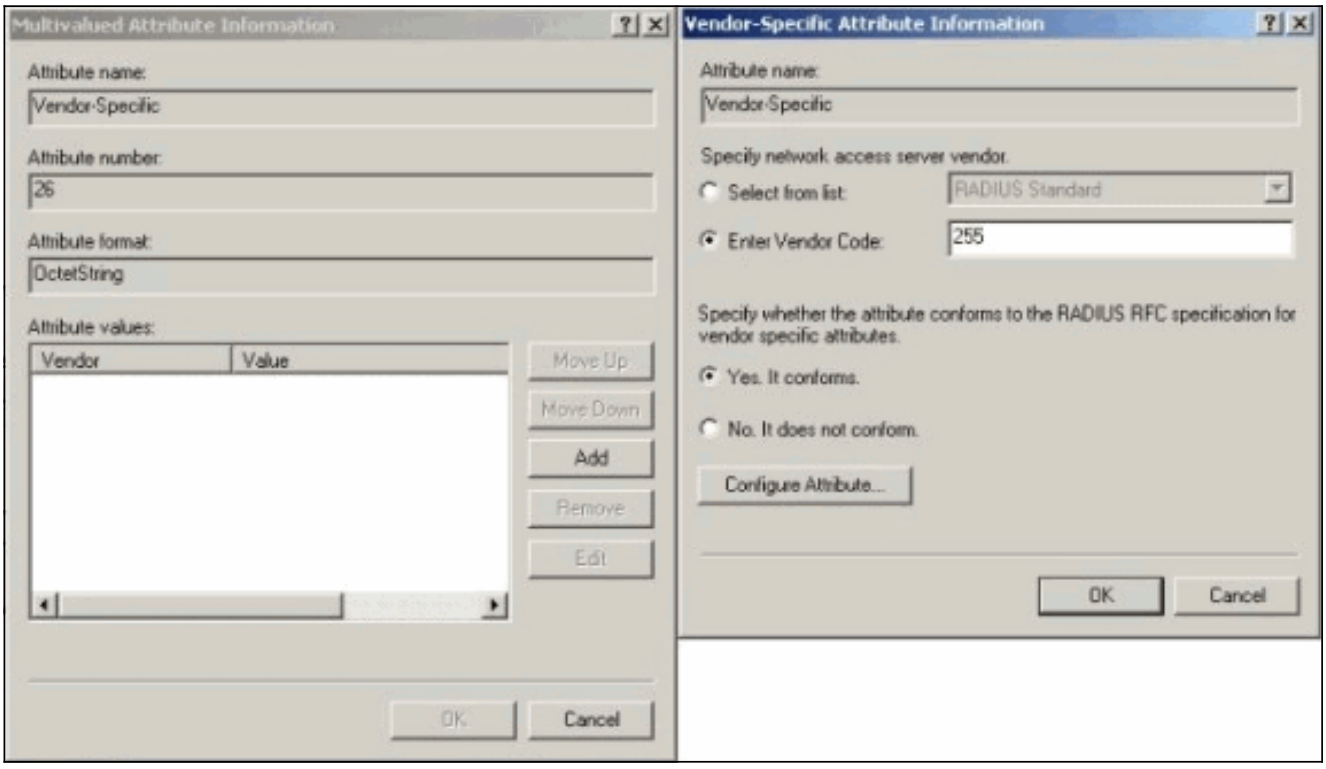


selecionado.

4. Selecione o guia avançada, o clique **adiciona** e seleciona **específico de fornecedor**.



5. Sob a caixa de diálogo Multivalued da informação de atributos para o atributo específico de fornecedor, o clique **adiciona** a fim ir à caixa de diálogo de informação de atributo específico de fornecedor. Seleto **dê entrada ao código de fornecedor** e incorpore **255 à** caixa adjacente. Seguinte, selecione **sim. Conforma-se** e o clique **configura o atributo**.

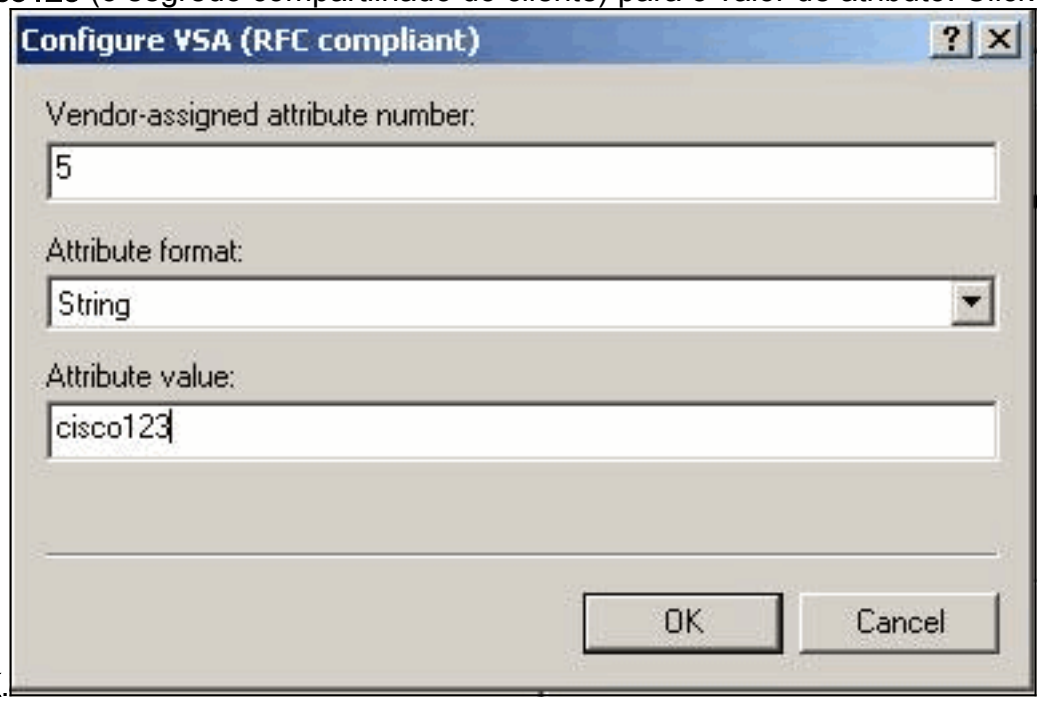


6. Sob a caixa de diálogo configurar VSA (em conformidade com RFC), incorpore **4** para o número de atributo Vendedor-atribuído, entre na **corda** para o formato de atributo, e

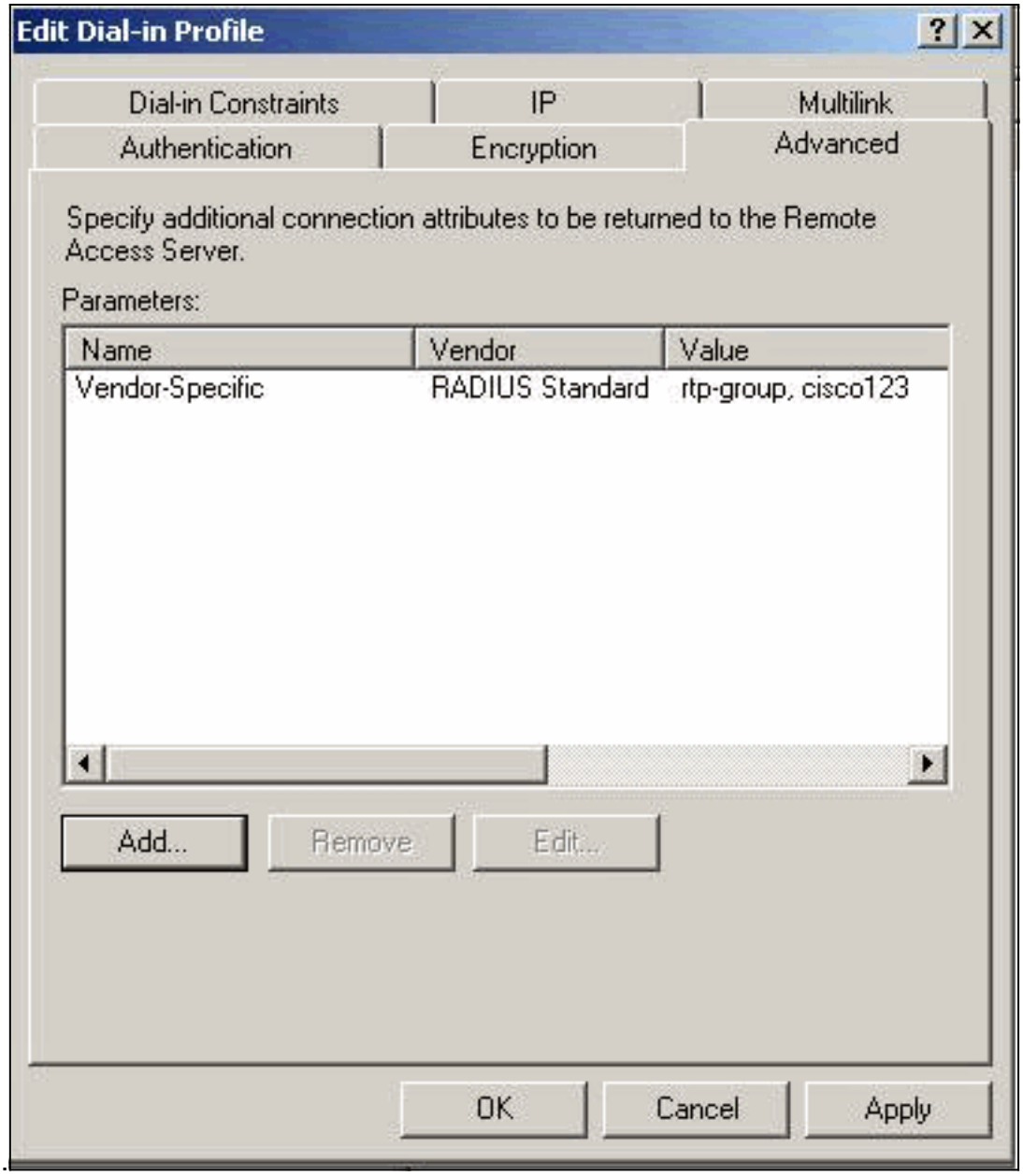
incorpore o RTP-**grupo** (nome do grupo de VPN no concentrador do Cisco VPN 5000) para o valor de atributo. Clique a **APROVAÇÃO** e repita a etapa

5. 

7. Sob a caixa de diálogo configurar VSA (em conformidade com RFC), incorpore **4** para o número de atributo Vendedor-atribuído, entre na **corda** para o formato de atributo, e entre no **cisco123** (o segredo compartilhado do cliente) para o valor de atributo. Click **OK**.



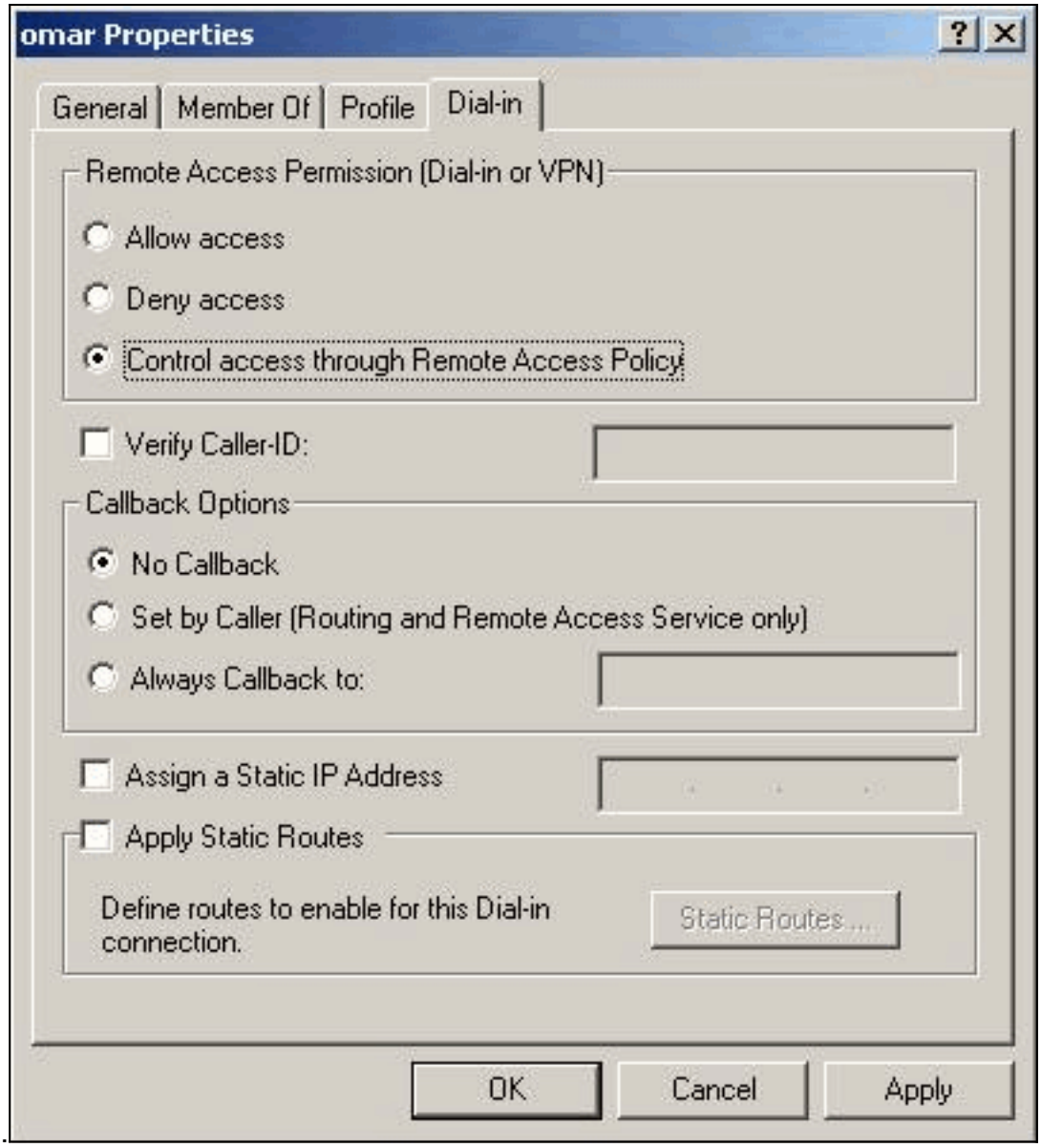
8. Você vê que o atributo específico de fornecedor contém dois valores (grupo e senha de



VPN).

9. Sob suas propriedades de usuário, clique o guia de discagem de entrada e assegure-se de que o **acesso do controle com a política de acesso remoto** esteja

selecionado.



Verifique o resultado

Esta seção fornece informações que você pode usar para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

- **mostre a visores de estatística do raio** estatísticas de pacote para uma comunicação entre o concentrador VPN e o server do raio padrão identificados pela seção do RAIO.
- **mostre a configuração do raio** — Mostra as configurações atual para parâmetros radius.

Esta é a saída do **comando show radius statistics**.

```
VPN5001_4B9CBA80>show radius statistics

RADIUS Stats

Accounting              Primary       Secondary
Requests                   0             na
Responses                  0             na
```

```
Retransmissions           0             na
Bad Authenticators        0             na
Malformed Responses       0             na
Packets Dropped           0             na
Pending Requests          0             na
Timeouts                  0             na
Unknown Types             0             na


Authentication         Primary       Secondary
Requests                  3             na
Accepts                   3             na
Rejects                   0             na
Challenges                0             na
Retransmissions           0             na
Bad Authenticators        0             na
Malformed Responses       0             na
Packets Dropped           0             na
Pending Requests          0             na
Timeouts                  0             na
Unknown Types             0             na



VPN5001_4B9CBA80>
```

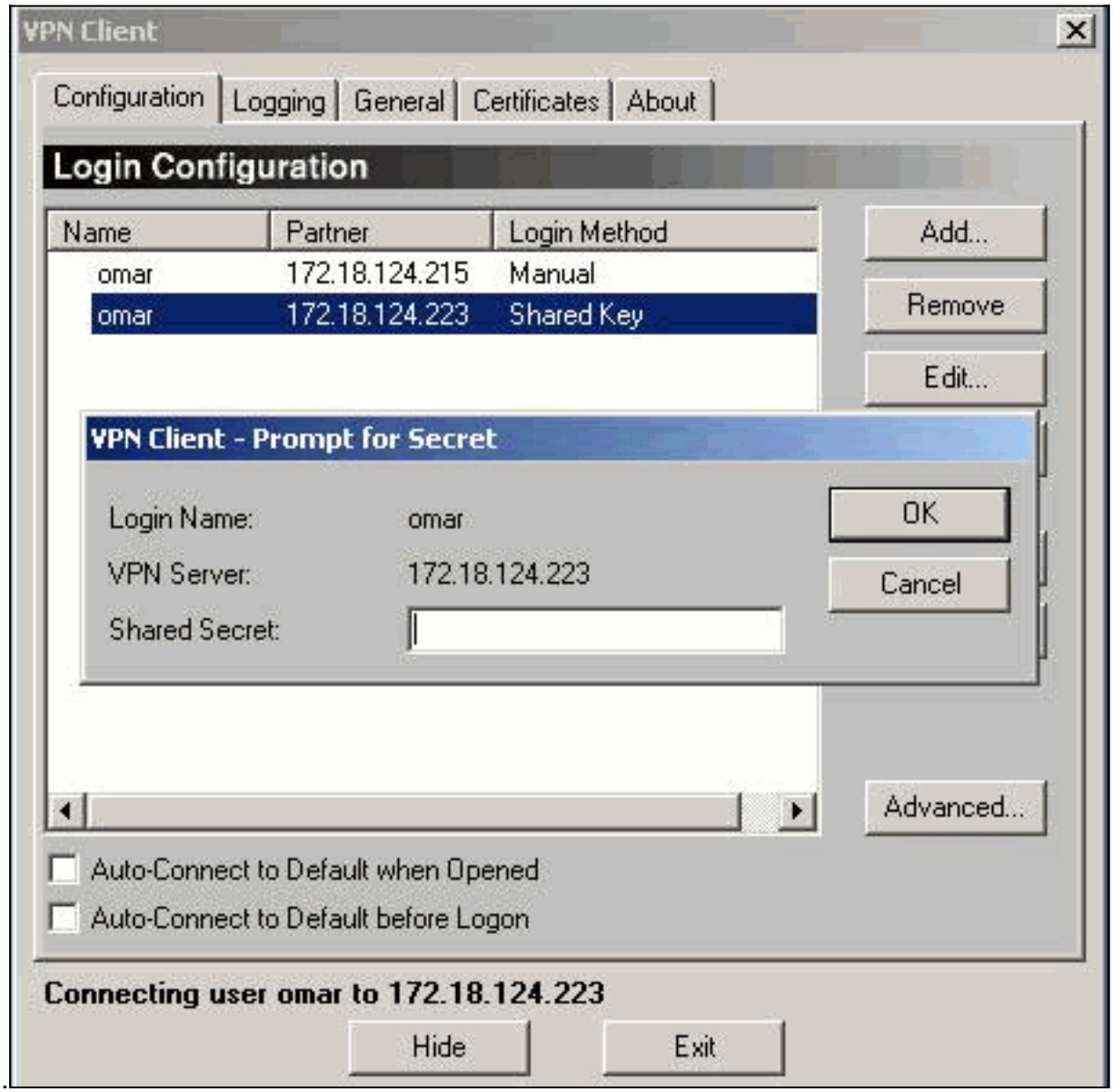
Esta é a saída do **comando show radius config**.

```
VPN5001_4B9CBA80>show radius statistics

RADIUS Stats

Accounting             Primary       Secondary
Requests                  0             na
Responses                 0             na
Retransmissions           0             na
Bad Authenticators        0             na
Malformed Responses       0             na
Packets Dropped           0             na
Pending Requests          0             na
Timeouts                  0             na
Unknown Types             0             na


Authentication         Primary       Secondary
Requests                  3             na
Accepts                   3             na
Rejects                   0             na
Challenges                0             na
Retransmissions           0             na
Bad Authenticators        0             na
Malformed Responses       0             na
Packets Dropped           0             na
Pending Requests          0             na
Timeouts                  0             na
Unknown Types             0             na



VPN5001_4B9CBA80>
```

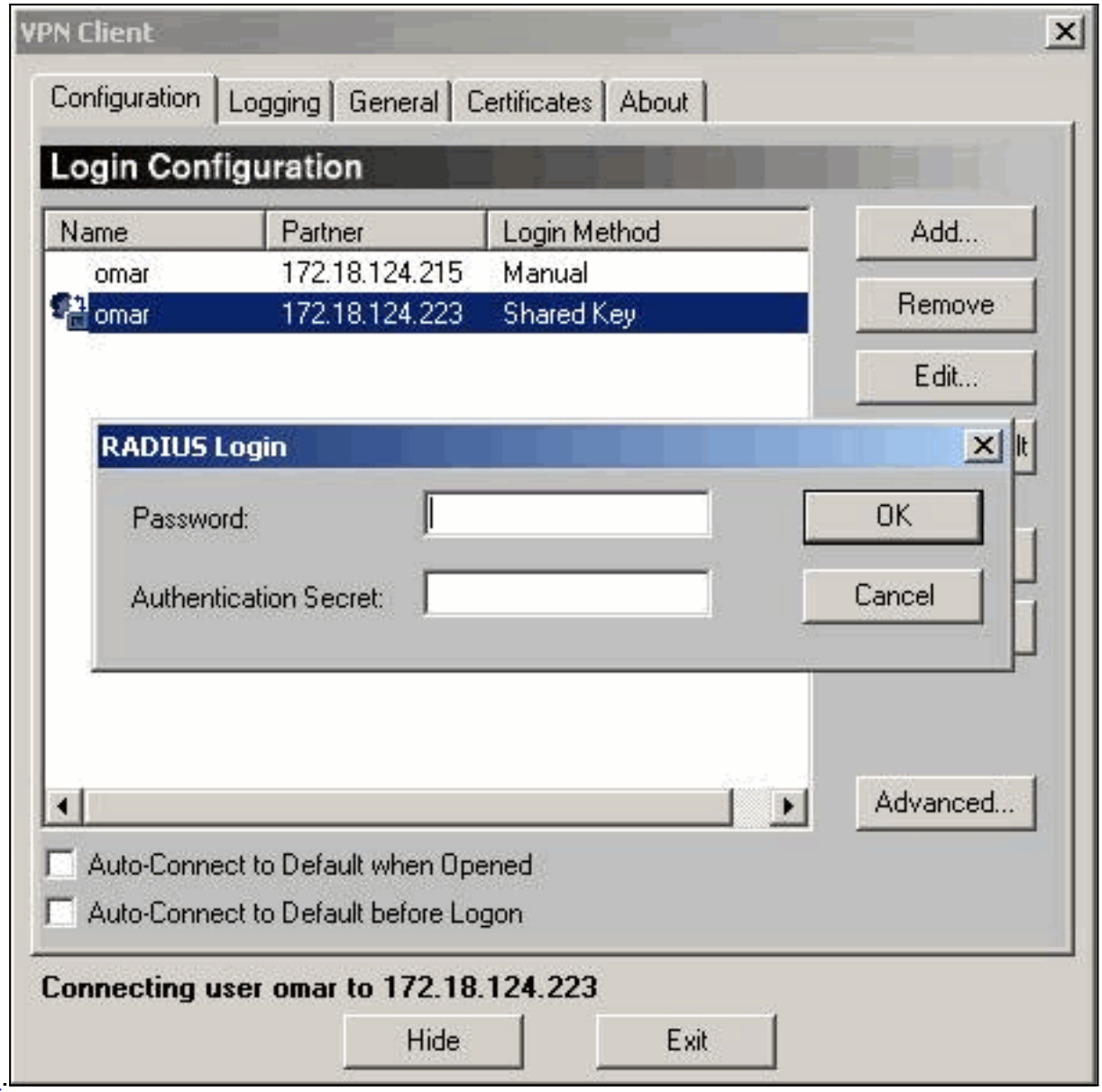
Configurar o VPN Client

Este procedimento guia-o com a configuração do cliente VPN.

1. Da caixa de diálogo do cliente VPN, selecione o guia de configuração. Em seguida, da Cliente-alerta VPN para a caixa de diálogo secreta, incorpore o segredo compartilhado sob o servidor de VPN. O segredo compartilhado cliente VPN é o valor incorporado para a senha de VPN do atributo 5 no concentrador VPN.



2. Depois que você incorpora o segredo compartilhado, você está alertado para uma senha e um segredo de autenticação. A senha é sua senha de radius para esse usuário, e o segredo de autenticação é o segredo da autenticação pap na seção do `[RADIUS] do` concentrador



VPN.

Registros do concentrador

```
VPN5001_4B9CBA80>show radius statistics

RADIUS Stats

Accounting            Primary       Secondary
Requests                 0             na
Responses                0             na
Retransmissions          0             na
Bad Authenticators       0             na
Malformed Responses      0             na
Packets Dropped          0             na
Pending Requests         0             na
Timeouts                 0             na
Unknown Types            0             na


Authentication        Primary       Secondary
Requests                 3             na
Accepts                  3             na
Rejects                  0             na
```

```
Challenges              0            na
Retransmissions         0            na
Bad Authenticators      0            na
Malformed Responses     0            na
Packets Dropped         0            na
Pending Requests        0            na
Timeouts                0            na
Unknown Types           0            na


VPN5001_4B9CBA80>
```

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Anúncio End-of-Life de concentradores do Cisco VPN 5000 Series
- Página de suporte do Cisco VPN 5000 Concentrator
- Página de suporte ao cliente do Cisco VPN 5000
- Página de suporte do IPSec
- Suporte Técnico - Cisco Systems