# Exemplo de Configuração de Roteador que Permite Clientes VPN se Conectarem via IPsec e à Internet Usando a Separação de Túneis

## Índice



## Introdução

Este documento fornece instruções passo a passo em como permitir o acesso de clientes VPN ao Internet quando forem escavados um túnel em um roteador de Cisco IOS®. Esta configuração é exigida para permitir que os Clientes VPN acessem com segurança recursos corporativos através do IPsec e, ao mesmo tempo, para permitir o acesso não protegido à Internet. Esta configuração é chamada tunelamento dividido.

**Nota:** O Split Tunneling pode levantar um risco de segurança quando configurado. Desde que os clientes VPN têm o acesso inseguro ao Internet, podem ser comprometidos por um atacante. Esse atacante pode então alcançar a LAN corporativa através do túnel de IPsec. Um acordo entre o Tunelamento e o Split Tunneling completos pode ser permitir a clientes VPN o acesso do LAN local somente. Refira ao PIX/ASA 7.x: Permita o acesso do LAN local para o exemplo de configuração dos clientes VPN para mais informação.

## Pré-requisitos

### Requisitos

Não existem requisitos específicos para este documento.

## Componentes Utilizados

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

- Roteador Cisco 3640 com Cisco IOS Software Release 12.4
- Cisco VPN Client 4.8

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

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

# Informações de Apoio

Os acessos remoto VPN endereçam a exigência da força de trabalho móvel conectar firmemente à rede da organização. Os usuários móveis podem estabelecer uma conexão segura usando o software do cliente VPN instalado em seus PC. O cliente VPN inicia uma conexão a um dispositivo da instalação central configurado para aceitar estes pedidos. Neste exemplo, o dispositivo da instalação central é um roteador do Cisco IOS que use mapas cripto dinâmico.

Quando você permite o Split Tunneling para conexões de VPN, exige a configuração de um Access Control List (ACL) no roteador. Neste exemplo, o **comando access-list 101** é associado com o grupo para finalidades do Split Tunneling, e o túnel é formado à rede 10.10.10.x/24. Os fluxos de tráfego não criptografado (por exemplo, o Internet) aos dispositivos são excluídos das redes configuradas no ACL 101.

```
access-list 101 permit ip 10.10.10.0 0.0.0.255 192.168.1.0 0.0.0.255
```

Aplique o ACL em propriedades do grupo.

```
crypto isakmp client configuration group vpngroup
 key cisco123
 dns 10.10.10.10
 wins 10.10.10.20
 domain cisco.com
 pool ippool
 acl 101
```

Neste exemplo de configuração, um túnel de IPsec é configurado com estes elementos:

- Crypto map aplicados às interfaces externas no PIX
- Autenticação extendida (XAUTH) dos clientes VPN contra uma autenticação local
- Atribuição dinâmica de um endereço IP privado de um pool aos clientes VPN
- A funcionalidade do **comando nat 0 access-list**, que permite que os anfitriões em um LAN usem endereços IP privados com um usuário remoto e ainda consigam um endereço do Network Address Translation (NAT) do PIX visitar uma rede não confiável.

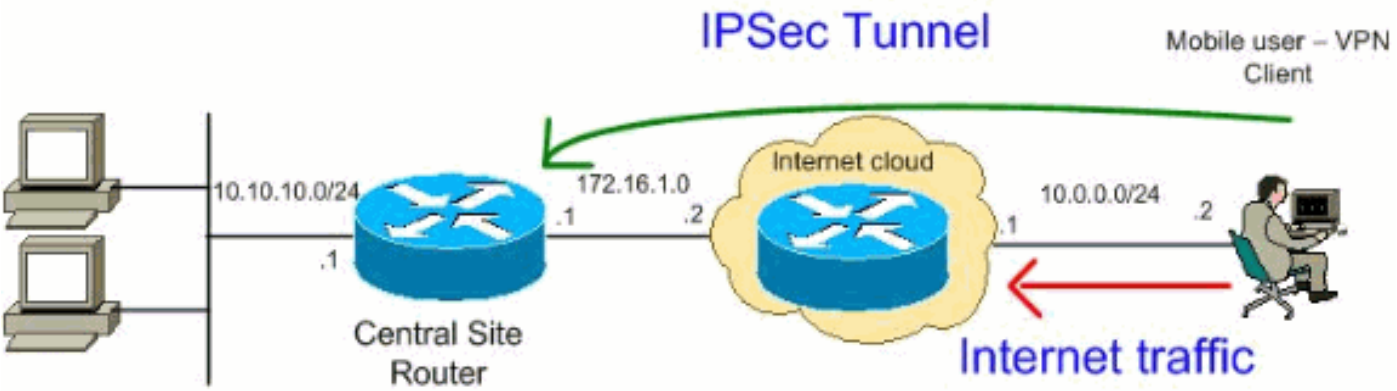
# Configurar

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

**Nota:** Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

## Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:




**Nota:** Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços da RFC1918 que foram usados em um ambiente de laboratório.

## Configurações

Este documento utiliza as seguintes configurações:

- Router
- Cisco VPN Client

**Router**

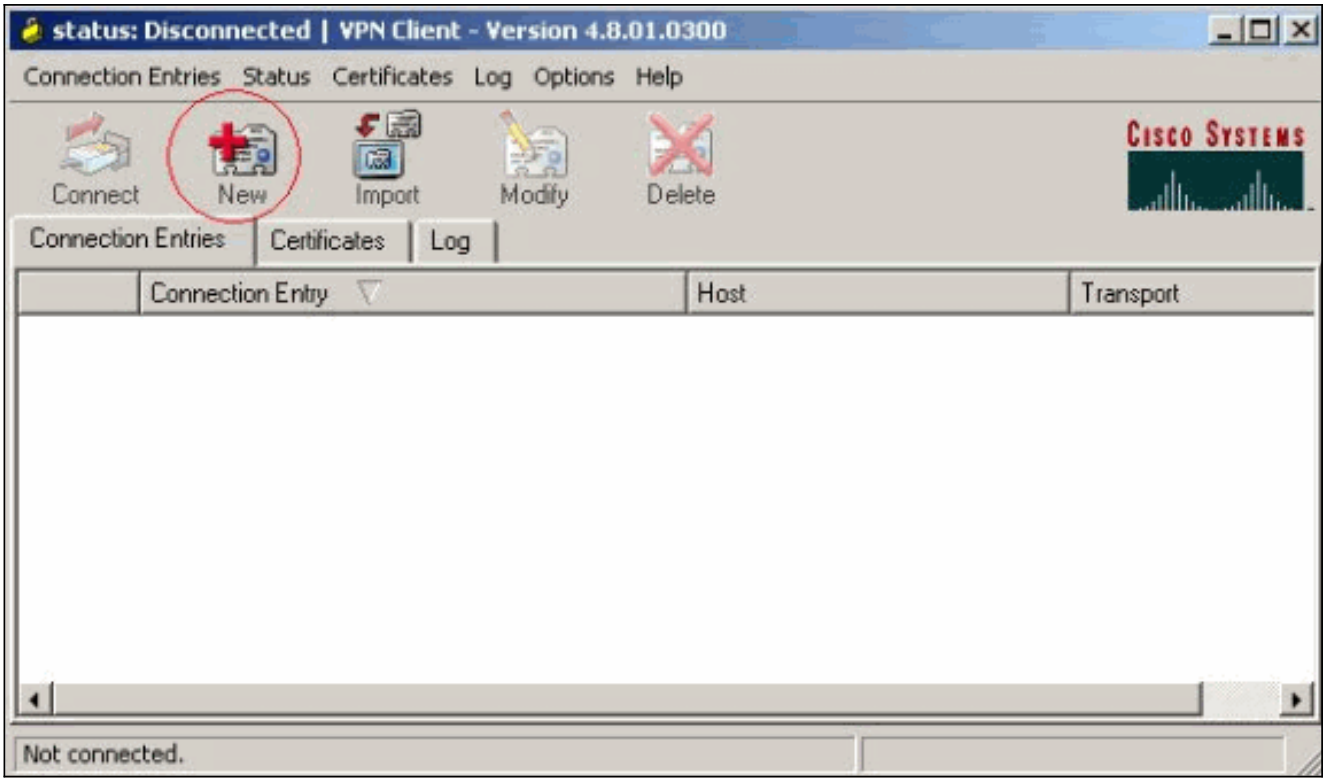
```
VPN#show run Building configuration... Current
configuration : 2170 bytes ! version 12.4 service
timestamps debug datetime msec service timestamps log
datetime msec no service password-encryption ! hostname
VPN ! boot-start-marker boot-end-marker ! ! !--- Enable
authentication, authorization and accounting (AAA) !---
for user authentication and group authorization. aaa
new-model ! !--- In order to enable Xauth for user
authentication, !--- enable the aaa authentication
commands. aaa authentication login userauthen local !---
In order to enable group authorization, enable !--- the
aaa authorization commands. aaa authorization network
groupauthor local ! aaa session-id common ! resource
policy ! ! !--- For local authentication of the IPsec
user, !--- create the user with a password. username
user password 0 cisco ! ! ! !--- Create an Internet
Security Association and !--- Key Management Protocol
(ISAKMP) policy for Phase 1 negotiations. crypto isakmp
policy 3 encr 3des authentication pre-share group 2 !---
Create a group that is used to specify the !--- WINS and
DNS server addresses to the VPN Client, !--- along with
the pre-shared key for authentication. Use ACL 101 used
```

```
for !--- the Split tunneling in the VPN Clinet end.
crypto isakmp client configuration group vpnclient key
cisco123 dns 10.10.10.10 wins 10.10.10.20 domain
cisco.com pool ippool acl 101 ! !--- Create the Phase 2
Policy for actual data encryption. crypto ipsec
transform-set myset esp-3des esp-md5-hmac ! !--- Create
a dynamic map and apply !--- the transform set that was
created earlier. crypto dynamic-map dynmap 10 set
transform-set myset reverse-route ! !--- Create the
actual crypto map, !--- and apply the AAA lists that
were created earlier. crypto map clientmap client
authentication list userauthen crypto map clientmap
isakmp authorization list groupauthor crypto map
clientmap client configuration address respond crypto
map clientmap 10 ipsec-isakmp dynamic dynmap ! ! ! !
interface Ethernet0/0 ip address 10.10.10.1
255.255.255.0 half-duplex ip nat inside !--- Apply the
crypto map on the outbound interface. interface
FastEthernet1/0 ip address 172.16.1.1 255.255.255.0 ip
nat outside ip virtual-reassembly duplex auto speed auto
crypto map clientmap ! interface Serial2/0 no ip address
! interface Serial2/1 no ip address shutdown ! interface
Serial2/2 no ip address shutdown ! interface Serial2/3
no ip address shutdown !--- Create a pool of addresses
to be !--- assigned to the VPN Clients. ! ip local pool
ippool 192.168.1.1 192.168.1.2 ip http server no ip http
secure-server ! ip route 0.0.0.0 0.0.0.0 172.16.1.2 !---
Enables Network Address Translation (NAT) !--- of the
inside source address that matches access list 111 !---
and gets PATed with the FastEthernet IP address. ip nat
inside source list 111 interface FastEthernet1/0
overload ! !--- The access list is used to specify which
traffic !--- is to be translated for the outside
Internet. access-list 111 deny ip 10.10.10.0 0.0.0.255
192.168.1.0 0.0.0.255 access-list 111 permit ip any any
!--- Configure the interesting traffic to be encrypted
from the VPN Client !--- to the central site router
(access list 101). !--- Apply this ACL in the ISAKMP
configuration. access-list 101 permit ip 10.10.10.0
0.0.0.255 192.168.1.0 0.0.0.255 control-plane ! line con
0 line aux 0 line vty 0 4 ! end
```

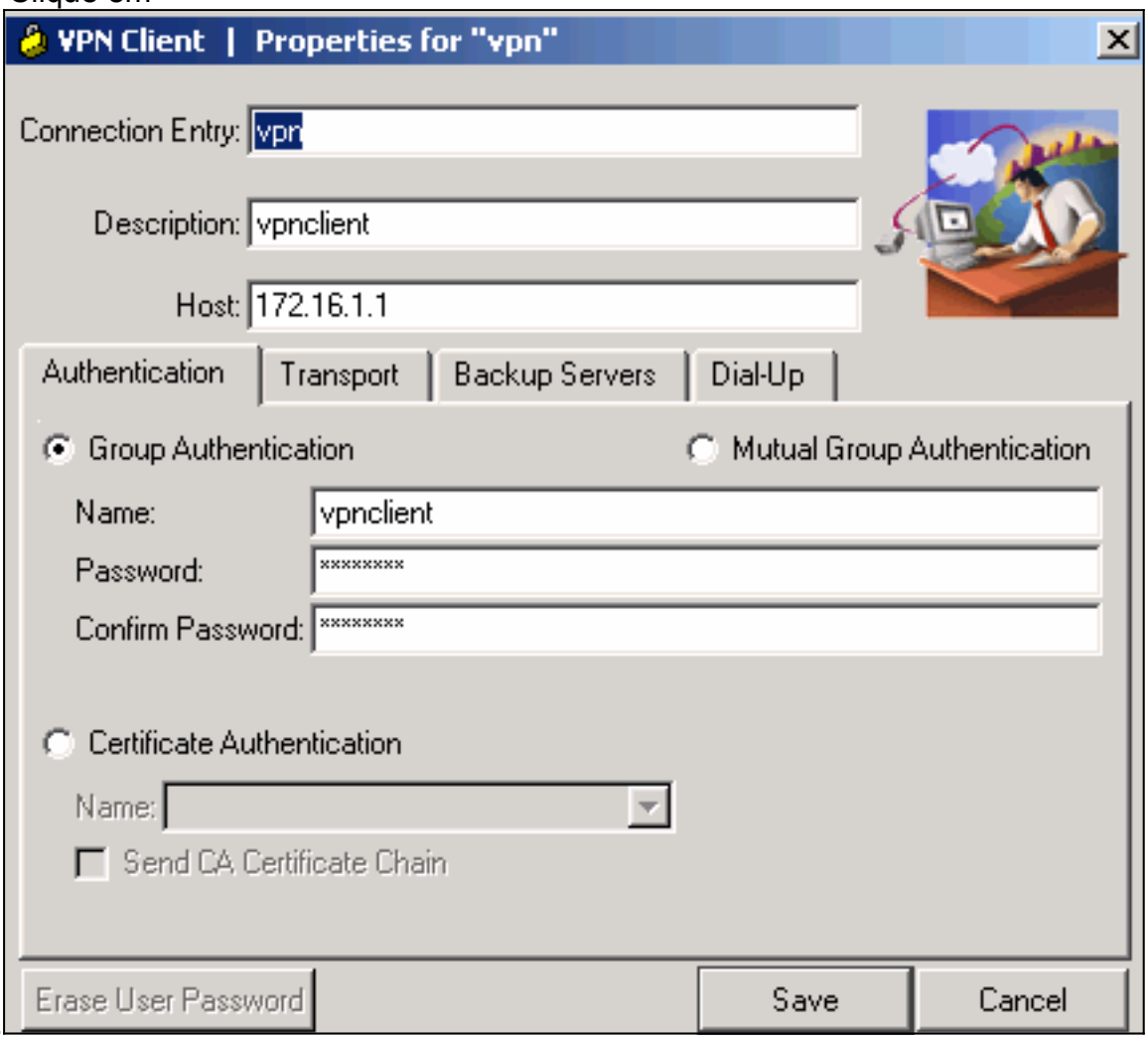
## Configuração do cliente VPN 4.8

Termine estas etapas a fim configurar o cliente VPN 4.8.

1. Escolha o **Iniciar > Programas > Cliente de VPN de Sistemas Cisco > o cliente VPN**.
2. Clique **novo** a fim lançar a janela de entrada nova da conexão de VPN da criação.

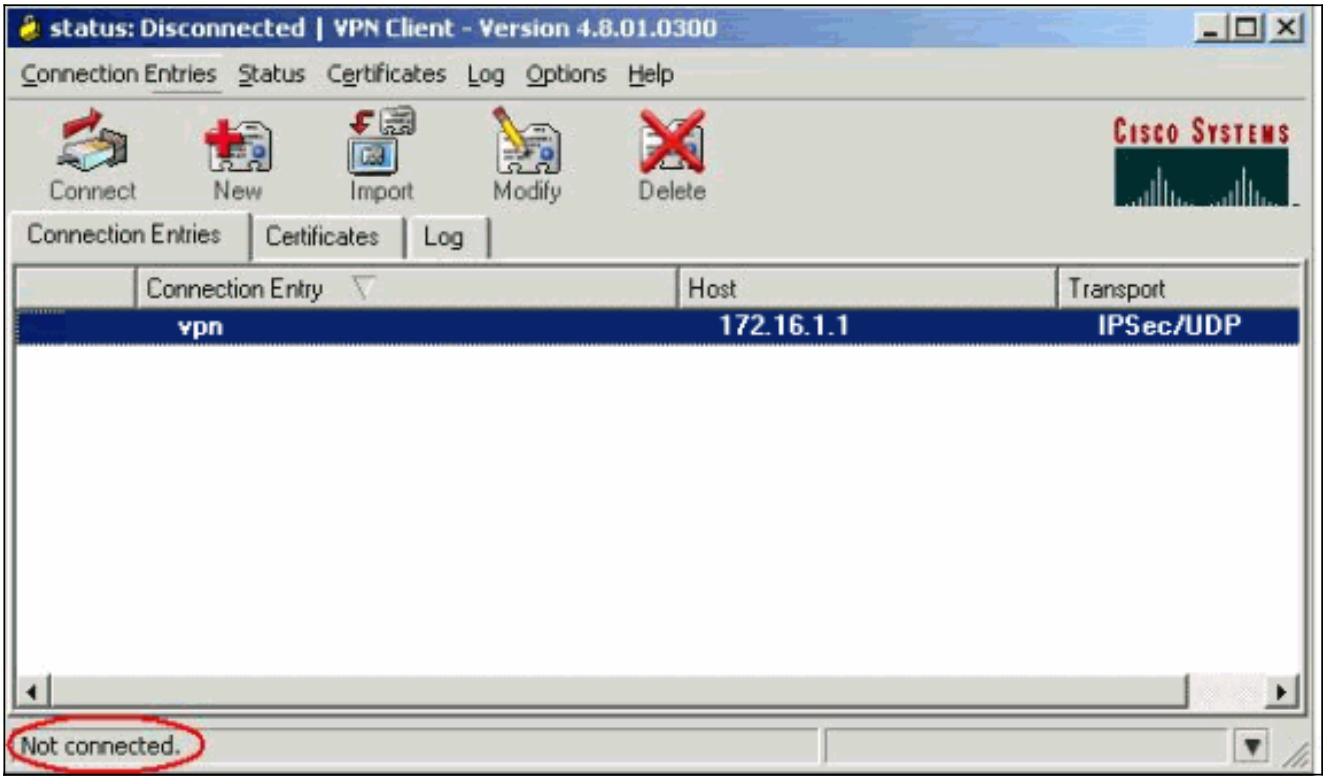



3. Dê entrada com o nome da entrada de conexão junto com uma descrição, incorpore o endereço IP externo do roteador à caixa do host, e incorpore o nome do grupo VPN e a senha. Clique em Salvar.



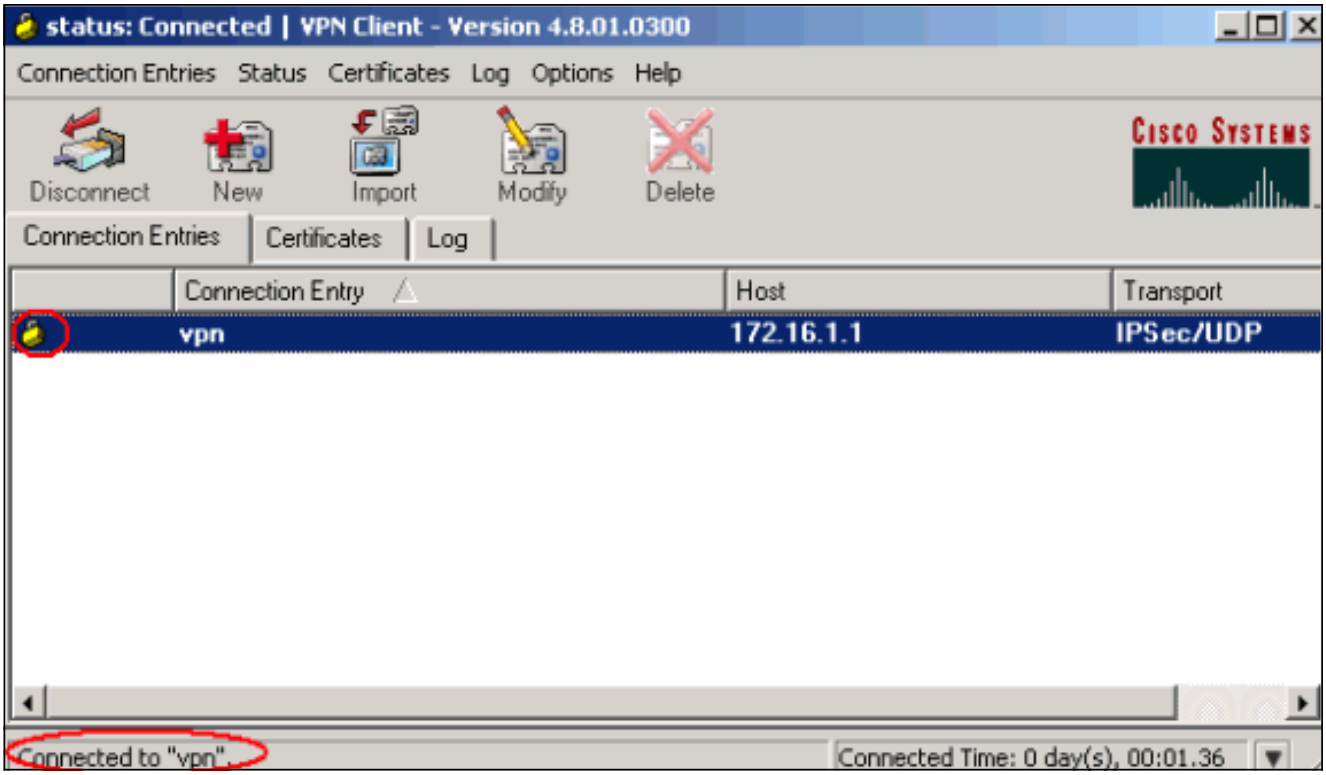

4. Clique sobre a conexão que você gostaria de se usar e o clique **conecta da** janela principal do cliente

VPN.

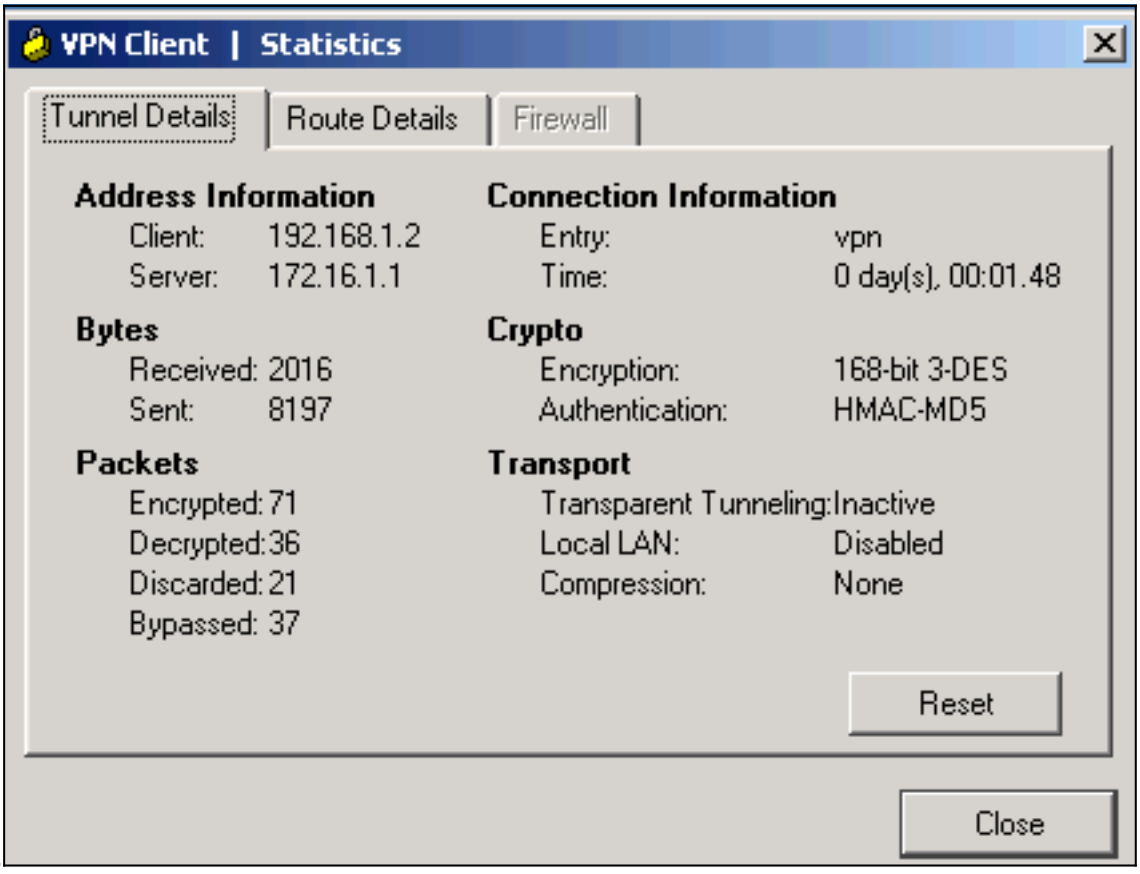



5. Quando alertado, incorpore a informação do nome de usuário e senha para o Xauth e clique a **APROVAÇÃO** a fim conectar à rede remota.

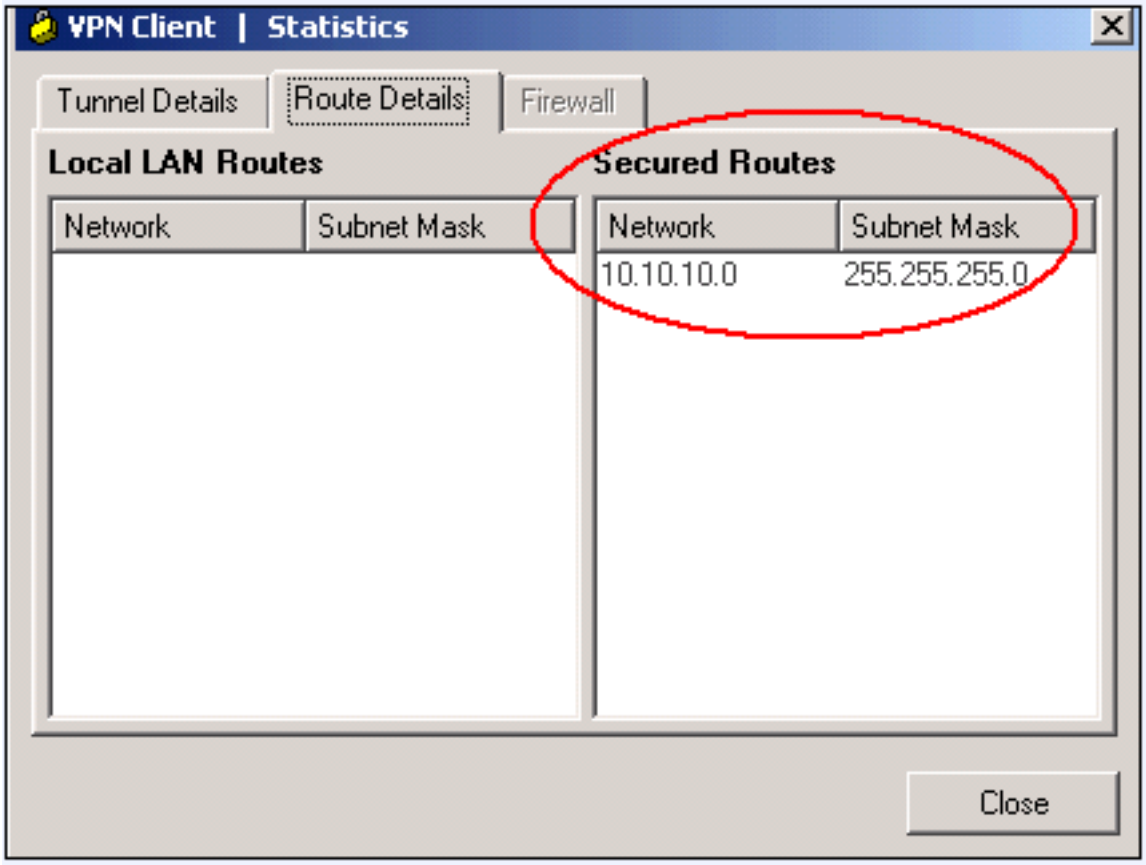

6. O cliente VPN obtém conectado com o roteador na instalação central.




7. Escolha o **estado > as estatísticas** a fim verificar as estatísticas do túnel do cliente VPN.




8. Vá à aba dos detalhes da rota a fim ver as rotas que o cliente VPN fixa ao roteador.Neste exemplo, o cliente VPN fixa o acesso a 10.10.10.0/24 quando todo tráfego restante não for cifrado e não é enviado através do túnel. A rede assegurada é transferida do ACL 101 que é configurada no roteador de site

central. 


## Verificar

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

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- show crypto isakmp sa – Mostra todas as associações de segurança (SAs) IKE atuais no correspondente.`VPN#show crypto ipsec sa interface: FastEthernet1/0 Crypto map tag: clientmap, local addr 172.16.1.1 protected vrf: (none) local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0) current_peer 10.0.0.2 port 500 PERMIT, flags={} #pkts encaps: 270, #pkts encrypt: 270, #pkts digest: 270 #pkts decaps: 270, #pkts decrypt: 270, #pkts verify: 270 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0 #pkts not decompressed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors 0 local crypto endpt.: 172.16.1.1, remote crypto endpt.: 10.0.0.2 path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet1/0 current outbound spi: 0xEF7C20EA(4017889514) inbound esp sas: spi: 0x17E0CBEC(400608236) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } conn id: 2001, flow_id: SW:1, crypto map: clientmap sa timing: remaining key lifetime (k/sec): (4530341/3288) IV size: 8 bytes replay detection support: Y Status: ACTIVE inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0xEF7C20EA(4017889514) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } conn id: 2002, flow_id: SW:2, crypto map: clientmap sa timing: remaining key lifetime (k/sec): (4530354/3287) IV size: 8 bytes replay detection support: Y Status: ACTIVE outbound ah sas: outbound pcp sas:`
- **mostre IPsec cripto sa** — Mostra os ajustes usados por SA atuais.`VPN#show crypto isakmp sa dst src state conn-id slot status 172.16.1.1 10.0.0.2 QM_IDLE 15 0 ACTIVE`

## Troubleshooting

## Comandos para Troubleshooting

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

**Nota:** Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

- **IPsec do debug crypto** — Indica as negociações de IPSEC de fase 2.
- debug crypto isakmp — Exibe as negociações ISAKMP da Fase 1.

# Informações Relacionadas

- Negociação IPsec/Protocolos IKE
- Cisco VPN Client - Sustentação do produto
- Roteador Cisco - Sustentação do produto
- Suporte Técnico e Documentação - Cisco Systems